The Insolvability of Polynomials of Degree 5 and above

By KJ Tim McDonald

Acknowledgments

I wish to thank the faculty and staff of the Department of Mathematics and Computer Science at Rutgers University - Newark, New Jersey campus for the rich mathematical experience they provided me during my graduate studies from 2003 to 2008, particularly to Dr. David Keys who introduced me to Galois theory, but especially to Dr. Robert Sczech who supervised my graduate Ph.D. thesis on p-adic number theory requiring a healthy dose of abstract algebra.

I also acknowledge the students of the many undergraduate courses I have taught both in New Jersey and Florida, experiences that have deepened my own understanding of how to communicate the beauty of mathematics. Two encounters stand out in that regard. First, a question one student asked : Why do mathematicians do research - isn't it all done? Second, a frustration on so many faces - these books are so hard to understand, yet I like math!

This book is dedicated to all of the above and in a different, particular way to my wife, Elizabeth, who has unwaveringly supported my life goal shift into the field of mathematics.

KJ Tim McDonald

May 8th, 2017

Preface

Our goal is to prove there are polynomial equations of degree ≥ 5 that are not solvable by radicals. This is most easily explained by attempting to derive formulas for finding the roots of polynomials of degrees 1,2,3 and 4 constructed by the usual mathematical operations of addition, subtraction, multiplication, division, taking n^{th} roots or radicals and raising to the n^{th} power. For example we have the quadratic formula for polynomials of degree 2,

$$\text{If } ax^2 + bx + c = 0 \text{ then } x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

We then prove that it is not possible to find such formulas for polynomials of a higher degree than 4 so we say they are not solvable by radicals.

The derivation of the formulas for polynomials of degree less than 5 involves only high school arithmetic and algebra, although the techniques used are very inventive. The proof that polynomials of degree greater than 4 are not solvable by radicals is much, much more difficult. It requires many of the tools and concepts of abstract algebra normally encountered in a demanding undergraduate course or a first year graduate course.

This book attempts to make this theory understandable by the ordinary reader, defined as a person interested in mathematics and skilled in introductory arithmetic and algebra theory to College Algebra level – of course some Calculus would enhance the reading experience. It is for a reader who wants to know a whole lot more about mathematics but doesn't want to spend several years acquiring the background to understand the proofs involved in the insolvability of polynomial equations of degree more than 4. The knowledge that reader will acquire is called abstract algebra covering groups to Galois Theory.

All of this exploration enables us to actually find polynomials of degree 5 that are not solvable by radicals as we say. An example is $f(x) = x^5 - 4x + 2$.

Classification of Degree of Difficulty of Theorems

Each Theorem is labelled with one to five stars thus,

Theorem*, Theorem**, ...,Theorem*****

indicating a degree of difficulty from,

*=Easy to *****= Very Hard or Very Long.

End Signals

The end of the proof of a Theorem is signaled with a box, □
The end of an Example of more than one line is signaled with a diamond, ◇.

Greek Alphabet Letters used in this Book

Letter	*Spoken as*
α	*alpha*
β	*beta*
γ	*gamma*
Δ, δ	*delta*
ϵ	*epsilon*
ζ	*zeta*
θ	*theta*
μ	*mu*
ξ	*xi*(*kigh*)
Π, π	*pi*
ρ	*rho*
Σ, σ	*sigma*
τ	*tau*
ϕ	*phi*
Ψ, ψ	*psi*(*sigh*)
Ω, ω	*omega*

Contents

Chapter 0

Notation and Definitions

0.1 Notation

Symbol	*Meaning*
$A = \{x, y, z, ...\}$	*A is the set of objects or elements* $x, y, z, ...$
$:$ *or* $\mid$	*such that*
$\forall$	*for all*
$\exists$	*there exists*
$x \in A$	x *is an element of set* A
$x \notin A$	x *is not an element of set* A
$A \cup B$	*the union of two sets* A *and* B
$A \cup B = \{x \mid x \in A$ *or* $x \in B\}$	*the union of two sets* A *and* B *is the set of* x *such that* x *is in* A *or* x *is in* B *(or both of them)*
$A \cap B$	*the intersection of two sets* A *and* B
$A \cap B = \{x \mid x \in A$ *and* $x \in B\}$	*the intersection of two sets* A *and* B *is the set of* x *such that* x *is in* A *and* x *is in* B
$A \subset B$	A *is contained within* B *or* A *is a subset of* B *that is, every element of* A *is also in* B
$A \supset B$	A *contains* B *or* B *is a subset of* A *that is, every element of* B *is also in* A
$A = B$	*Sets are equal if* $A \subset B$ *and* $A \supset B$ *–we say equality is double containment*
$f : A \to B$	*the function* f *maps the elements of the set* A *onto elements of the set* B
$\sum_{i=1}^{n} a_i$	$=$ *sum of* $a_1 + a_2 + \ldots + a_n$
$\prod_{i=1}^{n} a_i$	$=$ *product of* $a_1 a_2 \cdots a_n$
G	*usually means the group* G

$a \equiv b (\mathrm{mod}\ n)$	*a is congruent to b mod n*
$n \mid a$	*n divides a, that is,* $a = kn$
$\mathbb{Z}_n$	{0,1,2,. . . , n-1}, *the remainders when integers are divided by n*
$H \leq G$	*H is a subgroup of G and may be all of G*
$H < G$	*H is a proper subgroup of G*
$< a >$	*the cyclic group generated by a*
$\lvert G \rvert$	*the order of a group G.*
$\lvert a \rvert$	*the order of an element a of a group*
$f \circ g(x)$	*the composition of the two functions* $f(x)$ *and* $g(x)$
$f^{-1}(x)$	*the inverse function of* $f(x)$
S_n	*the symmetric group of permutations on* $(1, 2, ..., n)$
A_n	*the alternating group*
$ker(\phi)$	*kernel of a group function* ϕ
$G_1 \cong G_2$	*the groups* G_1 *and* G_2 *are isomorphic*
aH	*the coset of a subgroup H determined by a*
$[G : H]$	*the index of H in G or the number of left cosets of H in G*
$\mathbb{Q}^\times, \mathbb{R}^\times, \mathbb{C}^\times$	*the multiplicative groups* $\mathbb{Q} - \{0\}, \mathbb{R} - \{0\}, \mathbb{C} - \{0\}$
$H \lhd G$	*H is a normal subgroup of G*
$H \trianglelefteq G$	*H is a normal subgroup of G and may be all of G*
G/N	*the factor group of G on H*
$[a]_n$	*the set of integers with the same remainder when divided by n*
$\mathbb{Z}/n\mathbb{Z}$	*factor group of* $\mathbb{Z}$ *determined by* $n\mathbb{Z}$
$exp(G)$	*exponent of group G*
$F[x]$	*the set of polynomials in x with coefficients inF*
$< g(x) >$	*the set of all polynomials in* $F[x]$ *divisible by* $g(x)$
$p(x) \mid f(x)$	$p(x)$ *divides* $f(x)$, *or* $f(x) = p(x)q(x)$
$gcd(n, m)$	*greatest common divisor of integers m and n*
$gcd(f(x), g(x))$	*greatest common divisor of polynomials* $f(x)$ *and* $g(x)$
$[a(x)]_{p(x)}$	*the set of all polynomials in* $F[x]$ *with the same remainder* $a(x)$ *when divided by* $p(x)$
$F[x]/ < p(x) >$	*the set of possible remainders when a polynomial in* $F[x]$ *is divided by* $p(x)$
F/K	*F is an extension field of K*
$\mathfrak{B}$	*basis of a vector field*
$\mathbb{R}^n$	*the set of n – tuples of real numbers*
$[F : K]$	*the dimension of extension field F as a vector space over K*
$K(u)$	*a field K to which has been added the element* $u \notin K$
$Aut(F)$	*the group of automorphisms of F*
$Gal(F/K)$	*Galois group ofF/K or of the splitting field F of a polynomial* $f(x) \in K[x]$
F^G	*G – fixed subfield of field F*
$e^{\frac{2\pi i}{n}k}$	*an nth root of unity*

Logic Notation

If P and Q are statements we have,

Symbol	*Meaning*
$P \Rightarrow Q$	If P then Q or P implies Q
$P \Leftrightarrow Q$	P and Q are equivalent statements, or P implies Q and Q implies P

Number sets

There are six basic number sets: Natural Numbers $\mathbb{N}$, Integers $\mathbb{Z}$, Rationals $\mathbb{Q}$, Irrationals (numbers that can be placed on a number line but are not rationals, e.g. $\sqrt{2}$), Real Numbers $\mathbb{R}$ which are rationals plus irrationals, Complex numbers or numbers that are not real. They are defined as follows:

$$\mathbb{N} = \{1, 2, 3, \ldots\}$$
$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$$
$$\mathbb{Q} = \{\frac{a}{b} | a, b \in \mathbb{Z}, b \neq 0\}$$
$$Irrationals$$
$$\mathbb{R} = \mathbb{Q} \cup \{Irrationals\}$$
$$\mathbb{C} = \{a + bi | a, b \in \mathbb{R}, i = \sqrt{-1}\}$$

0.2 Definitions

Definition 1. *polynomial function and polynomial equation*
A polynomial function has the form,

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

A polynomial equation has the form,

$$f(x) = 0 \quad or \quad a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0$$

where in both cases $a_i \in \mathbb{R}$ for $i : 0 \leq i \leq n$ and $n \in \mathbb{N}$.

Definition 2. *coefficient of a polynomial*
Each $a_i, 0 \leq i \leq n$ of a polynomial is called a coefficient .

Definition 3. *degree of a polynomial*
The degree of a polynomial is the highest power of x. Accordingly,

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0, \ a_n \neq 0$$

has degree n.

Example 1. $2x^3 - 4x^2 + 11 = 0$ *is a polynomial equation of degree 3.*

Definition 4. *monic polynomial*
A monic polynomial of degree n has a leading coefficient $a_n = 1$.

Example 2. $f(x) = x^4 + 2x - 7$ *is a monic polynomial.*
We can always reduce a polynomial equation to its monic form by dividing through by a_n *to give new* $a_i's$ *as with* $2x^3 - 3x + 4 = 0 \Leftrightarrow x^3 - \frac{2}{3}x + 2 = 0$ $\diamond$

The values of x for which a polynomial $f(x)$ becomes zero are called the roots or zeros of the polynomial. Accordingly these values are the solutions of the polynomial equation $f(x) = 0$. Our goal is to find algebraic formulas for the roots or zeros of all polynomials of degree ≤ 4 and to prove no such formula exists for all polynomials of degree > 4 where the formulas use only the usual algebraic operations and the application of radicals or roots (square, cube, etc.). We begin with degree 1.

Chapter 1

Solving Polynomials Degree ≤ 4

1.1 Formula I: Solving Linear or degree 1 Equations

A monic linear equation has the form $x + b = 0$.
The single zero is $x = -b$ since $-b + b = 0$.

1.2 Formula II: Solving Quadratic or degree 2 Equations

A monic quadratic equation has the form $x^2 + bx + c = 0$

Rather than, as we do in a College Algebra course, completing the square on $ax^2 + bx + c = 0$ to obtain the quadratic formula for the two roots,

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a},$$

we will use a technique that generalizes to polynomial equations of degree 2, 3 and 4.

In all of these cases of polynomials degree $n = 2, 3, 4$, we eliminate the term in degree $n - 1$ by making the substitution $x = y - \frac{b}{n}$. For $x^2 + bx + c = 0$ we substitute $x = y - \frac{b}{2}$ to eliminate the term in y. We obtain,

$$\left(y - \frac{b}{2}\right)^2 + b\left(y - \frac{b}{2}\right) + c = 0$$
$$\Rightarrow y^2 - \cancel{by} + \frac{b^2}{4} + \cancel{by} - \frac{b^2}{2} + c = 0$$

This eliminates the term of degree 1.

$$\Rightarrow y^2 = \frac{b^2}{4} - c = \frac{b^2 - 4c}{4}$$
$$\Rightarrow y = \pm\frac{\sqrt{b^2 - 4c}}{2}$$
$$\Rightarrow x = y - \frac{b}{2} = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

Of course, if we apply this method to $ax^2 + bx + c = 0$ by substituting $x = y - \frac{b}{2a}$ we find,

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

The nature of the roots depends upon $b^2 - 4ac$ which is called the discriminant.

- If $b^2 - 4ac > 0$ there are two real roots
- If $b^2 - 4ac = 0$ there is one real root which is also a rational number since the polynomial was a perfect square of the form $(x - d)^2$.
- If $b^2 - 4ac < 0$ there are two complex roots

1.3 Formula III: Solving Cubic or degree 3 Equations

Given $x^3 + bx^2 + cx + d = 0$, we substitute $x = y - \frac{b}{3}$ to obtain,

$$\left(y - \frac{b}{3}\right)^3 + b\left(y - \frac{b}{3}\right)^2 + c\left(y - \frac{b}{3}\right) + d = 0$$
$$\Rightarrow y^3 - \cancel{3y^2\frac{b}{3}} + 3y\frac{b^2}{9} - \frac{b^3}{27} + \cancel{by^2} - \frac{2b^2y}{3} + \frac{b^3}{9} + cy - \frac{bc}{3} + d = 0$$
$$\Rightarrow y^3 + \left(c + \frac{b^2}{3}\right)y + \left(d + \frac{2b^3}{27} - \frac{bc}{3}\right) = 0$$
$$\Rightarrow y^3 + py + q = 0, \text{where } p = \left(c + \frac{b^2}{3}\right) \text{ and } q = \left(d + \frac{2b^3}{27} - \frac{bc}{3}\right)$$

This is called a reduced cubic with the term in degree 2 eliminated. We now follow the "trick" due to Vieta. The original solution is due to del Ferro (1465-1526) and Tartaglia (1500-1577). Substitute $y = w - \frac{p}{3w}$ which has the effect of eliminating the

two terms of degree 1 and 2. We obtain,

$$\begin{aligned}
\left(w - \frac{p}{3w}\right)^3 + p\left(w - \frac{p}{3w}\right) + q &= 0 \\
w^3 - \cancel{3w^2\frac{p}{3w}} + \cancel{3w\frac{p^2}{9w^2}} - \frac{p^3}{27w^3} + \cancel{pw} - \cancel{\frac{p^2}{3w}} + q &= 0 \\
\Rightarrow w^3 + q - \frac{p^3}{27w^3} &= 0 \\
\Rightarrow w^6 + qw^3 - \frac{p^3}{27} &= 0 \\
\Rightarrow (w^3)^2 + q(w^3) - \frac{p^3}{27} &= 0
\end{aligned}$$

This is a quadratic equation in w^3, so, using the quadratic formula and taking the plus sign, we have,

$$w^3 = \frac{-q + \sqrt{q^2 + \dfrac{4p^3}{27}}}{2} = Q, \ say.$$

Then the three roots[1] are,

$$w = \sqrt[3]{Q}, \quad w = \sqrt[3]{Q}e^{\frac{2\pi i}{3}}, \quad w = \sqrt[3]{Q}e^{\frac{4\pi i}{3}}$$

Here, we introduce the 3^{rd} roots of unity arguing,

$$w^3 = Q \times 1 \Rightarrow w = \sqrt[3]{1}\sqrt[3]{Q} \Rightarrow w = \sqrt[3]{Q}e^{\frac{k2\pi i}{3}}, \ k = 0, 1, 2$$

Note also that, using $e^{ix} = \cos x + i \sin x$,

$$\begin{aligned}
e^{\frac{2\pi i}{3}} &= \cos\frac{2\pi}{3} + i\sin\frac{2\pi i}{3} = \frac{-1 + \sqrt{3}i}{2} \\
e^{\frac{4\pi i}{3}} &= \cos\frac{4\pi}{3} + i\sin\frac{4\pi i}{3} = \frac{-1 - \sqrt{3}i}{2}
\end{aligned}$$

This means we have one real root and two complex (conjugate) roots, given by,

$$x = y - \frac{b}{3} = w - \frac{p}{3w} - \frac{b}{3}$$

where $p = \left(c + \dfrac{b^2}{3}\right), \ q = \left(d + \dfrac{2b^3}{27} - \dfrac{bc}{3}\right)$ and w has the three given values.

[1]Please consult the Appendix if you are unfamiliar with the exponential function and roots of unity, or simply, at this early stage, use the factoring of the difference of two cubes and the quadratic formula thus,

$$\begin{aligned}
&w^3 = Q \Rightarrow w^3 - (Q^{\frac{1}{3}})^3 = 0 \Rightarrow (w - Q^{\frac{1}{3}})(w^2 + wQ^{\frac{1}{3}} + Q^{\frac{2}{3}}) = 0 \\
&\Rightarrow w = Q^{\frac{1}{3}} \ \text{ or } \ w^2 + wQ^{\frac{1}{3}} + Q^{\frac{2}{3}} = 0 \\
&\Rightarrow w = Q^{\frac{1}{3}}, \ \frac{-Q^{\frac{1}{3}} \pm \sqrt{Q^{\frac{2}{3}} - 4Q^{\frac{2}{3}}}}{2} = Q^{\frac{1}{3}}, \ Q^{\frac{1}{3}}\left(\frac{-1 \pm \sqrt{3}i}{2}\right)
\end{aligned}$$

Example 3. *Find the zeros of the cubic equation,* $x^3 - 9x^2 + 36x - 80 = 0$
Solution *Here* $a = 1, b = -9, c = 36, d = -80$ *with respect to* $ax^3 + bx^2 + cx + d$.
Let $x = y - \frac{b}{3} = y - \frac{-9}{3} = y + 3$. *The resolvent cubic is,*

$$
\begin{aligned}
&(y+3)^3 - 9(y+3)^2 + 36(y+3) - 80 = 0\\
&\Rightarrow y^3 + \cancel{3y^2 3} + 3y9 + 27 - \cancel{9y^2} - 54y - 81 + 36y + 108 - 80 = 0\\
&\Rightarrow y^3 + 9y - 26 = 0\\
&\Rightarrow y^3 + py + q = 0,\ p = 9, q = -26, \textit{with the degree 2 term eliminated.}\\
&\textit{Substituting, } y = w - \frac{p}{3w} = w - \frac{9}{3w} = w - \frac{3}{w}\\
&\Rightarrow (w - \frac{3}{w})^3 + 9(w - \frac{3}{w}) - 26 = 0\\
&\Rightarrow w^3 - \cancel{3w^2\frac{3}{w}} + \cancel{3w\frac{9}{w^2}} - \frac{27}{w^3} + \cancel{9w} - \cancel{\frac{27}{w}} - 26 = 0\\
&\Rightarrow w^3 - 26 - \frac{27}{w^3} = 0\\
&\Rightarrow w^6 - 26w^3 - 27 = 0,\\
&\textit{which is a quadratic equation in } w^3.\\
&\Rightarrow w^3 = \frac{26 \pm \sqrt{676 + 108}}{2} = 13 \pm \sqrt{196} = -1, 27
\end{aligned}
$$

Then, using $w^3 = 27$ *we have*[2],

$$
\begin{aligned}
&w = 3 \text{ or } w = 3e^{\frac{2\pi i}{3}} \text{ or } w = 3e^{\frac{4\pi i}{3}}\\
&\Leftrightarrow w_1 = 3, w_2 = 3\left(\frac{-1 + i\sqrt{3}}{2}\right), w_3 = 3\left(\frac{-1 - i\sqrt{3}}{2}\right)
\end{aligned}
$$

giving these values for y :

$$
\begin{aligned}
y_1 &= w_1 - \frac{3}{w_1} = 3 - \frac{3}{3} = 2\\
y_2 &= w_2 - \frac{3}{w_2} = \frac{3(-1 + i\sqrt{3})}{2} - \frac{6}{3(-1 + \sqrt{3}i)}\\
&= \frac{-3 + 3i\sqrt{3}}{2} - 2\frac{-1 - i\sqrt{3}}{(-1 + i\sqrt{3})(-1 - i\sqrt{3})}\\
&= \frac{-3 + 3i\sqrt{3}}{2} - \frac{-1 - i\sqrt{3}}{2} = -1 + 2i\sqrt{3}\\
y_3 &= w_3 - \frac{3}{w_3} = \frac{3(-1 - i\sqrt{3})}{2} - \frac{6}{3(-1 - i\sqrt{3})}
\end{aligned}
$$

[2]Or see the previous footnote with $Q = 27$.

$$= \frac{-3-3i\sqrt{3}}{2} - 2\frac{-1+i\sqrt{3}}{(-1+i\sqrt{3})(-1-i\sqrt{3})}$$
$$= \frac{-3-3i\sqrt{3}}{2} - \frac{-1+i\sqrt{3}}{2} = -1-2i\sqrt{3}$$

Using $x_i = y_i + 3$ the solutions to our cubic equation are $5, 2+2\sqrt{3}i, 2-2\sqrt{3}i$.
Notice that the two complex roots are conjugates. ◇

If we use $w = -1$, we obtain the same three roots (your turn!). It is worth noting that the original mathematicians who solved the cubic did not have the advantage of complex numbers. Even more interesting, there are cubics whose zeros all appear to be complex numbers even though they are actually rationals, indeed integers. Let's do one more example.

Example 4. *Find the zeros of $x^3 - 7x - 6 = 0$*
Solution
Applying the Factor Theorem[3] to $f(x) = x^3 - 7x - 6$ we have,

$$f(-1) = (-1)^3 - 7(-1) - 6 = 0$$

so $x+1$ is a factor or -1 is a root.
By long or synthetic division we obtain,

$$x^3 - 7x - 6 = (x+1)(x^2 - x - 6) = (x+1)(x-3)(x+2)$$

Therefore the three roots of $x^3 - 7x - 6 = 0$ are $-1, -2, 3$.
It is, however, very enlightening to apply the method to this equation. We already have a resolvent cubic $x^3 + px + q = x^3 - 7x - 6$ with no x^2 term so we simply substitute (following Vieta), $x = w - \frac{p}{3w} = w + \frac{7}{3w}$ to obtain,

$$\left(w + \frac{7}{3w}\right)^3 - 7\left(w + \frac{7}{3w}\right) - 6 = 0$$
$$\Rightarrow w^3 + 3w^2\frac{7}{3w} + 3w\frac{49}{9w^2} + \frac{343}{27w^3} - 7w - \frac{49}{3w} - 6 = 0$$
$$\Rightarrow w^6 - 6w^3 + \frac{343}{27} = 0$$
$$\Rightarrow w^3 = \frac{6 \pm \sqrt{36 - \frac{1372}{27}}}{2} = \frac{6 \pm \sqrt{\frac{-400}{27}}}{2} = \frac{6 \pm 20\sqrt{\frac{-3}{81}}}{2} = 3 \pm \frac{10}{9}i\sqrt{3}$$
$$\Rightarrow w = \sqrt[3]{3 \pm \frac{10}{9}i\sqrt{3}}\ \ e^{\frac{k2\pi i}{3}},\ k = 0, 1, 2.$$

[3] $f(a) = 0 \Rightarrow (x-a)$ is a factor of $f(x)$. We prove this again in Corollary 55 on page 104.

If we take the positive sign and $k = 0$ then the corresponding value of x is given by,

$$x = w + \frac{7}{3w} = \sqrt[3]{3 + \frac{10}{9}i\sqrt{3}} + \frac{7}{\sqrt[3]{3 + \frac{10}{9}i\sqrt{3}}}$$

This root seems a long way removed from -1, -2 or 3. This is the dilemma that confronted Tartaglia, del Ferro and the other contributors. In the previous example we did immediately find one real root so they were satisfied with that, knowing nothing about complex numbers, but in this current example there seemed no way out for Tartaglia et. al. We, however, can proceed as follows to find the cube root. Let,

$$3 + \frac{10}{9}i\sqrt{3} = (a + bi)^3 = a^3 + 3a^2bi - 3ab^2 - b^3i$$

Comparing real and imaginary parts we have the two equations in two unknowns,

$$\begin{aligned} a^3 - 3ab^2 &= 3 \\ 3a^2b - b^3 &= \frac{10}{9}\sqrt{3} \end{aligned}$$

It is clear from the second equation that b has $\sqrt{3}$ as a factor. If we then use trial and error, we eventually find $a = \frac{9}{6}$, $b = \frac{\sqrt{3}}{6}$ so the three values of w resulting from $w^3 = 3 + \frac{10}{9}i\sqrt{3}$ are,

$$w = \frac{9 + \sqrt{3}i}{6} e^{\frac{k2\pi i}{3}}, k = 0, 1, 2$$

So, using, $e^{\frac{2\pi i}{3}} = \left(\frac{-1 + i\sqrt{3}}{2}\right)$, $e^{\frac{4\pi i}{3}} = \left(\frac{-1 - i\sqrt{3}}{2}\right)$, we have the three values of w,

$$\begin{aligned} w_1 &= \frac{9 + \sqrt{3}i}{6} \\ w_2 &= \left(\frac{9 + \sqrt{3}i}{6}\right)\left(\frac{-1 + \sqrt{3}i}{2}\right) = \frac{-3 + 2\sqrt{3}i}{3}, \\ w_3 &= \left(\frac{9 + \sqrt{3}i}{6}\right)\left(\frac{-1 - \sqrt{3}i}{2}\right) = \frac{-3 - 5\sqrt{3}i}{6}, \end{aligned}$$

Then the three roots resulting from $x = w + \dfrac{7}{3w}$ *are,*

$$\begin{aligned}
x_1 &= \frac{9+\sqrt{3}i}{6} + \frac{7}{\cancel{3}} \bullet \frac{\cancel{6}2}{9+\sqrt{3}i} \bullet \frac{9-\sqrt{3}i}{9-\sqrt{3}i} \\
&= \frac{9+\sqrt{3}i}{6} + \cancel{14}\left(\frac{9-\sqrt{3}i}{\cancel{81+3}\ 6}\right) = 3 \\
x_2 &= \frac{-3+2\sqrt{3}i}{3} + \frac{7}{\cancel{3}} \bullet \frac{\cancel{3}}{-3+2\sqrt{3}i} \bullet \frac{-3-2\sqrt{3}i}{-3-2\sqrt{3}i} \\
&= \frac{-3+2\sqrt{3}i}{3} + \cancel{7}\left(\frac{-3-2\sqrt{3}i}{\cancel{9+12}\ 3}\right) = -2 \\
x_3 &= \frac{-3-5\sqrt{3}i}{6} + \frac{7}{\cancel{3}} \bullet \frac{\cancel{6}\ 2}{-3-5\sqrt{3}i} \bullet \frac{-3+5\sqrt{3}i}{-3+5\sqrt{3}i} \\
&= \frac{-3-5\sqrt{3}i}{6} + \cancel{14}\left(\frac{-3+5\sqrt{3}i}{\cancel{9+75}\ 6}\right) = -1
\end{aligned}$$

If we started with the other value $w^3 = 3 - \dfrac{10}{9}i\sqrt{3}$ *we would find the same roots.* $\diamond$

Proofs of this kind that required complex numbers were obviously contraversial when first used in finding the solutions of polynomials with real roots.

1.4 Formula IV: Solving Quartic or degree 4 Equations

The first step in solving a polynomial equation of the form,

$$x^4 + bx^3 + cx^2 + dx + e = 0$$

is the same idea, namely, substitute $x = y - \dfrac{b}{4}$ and eliminate the term in y^3 thus,

$$\begin{aligned}
y^4 - \cancel{4y^3}\frac{b}{4} + 6y^2\frac{b^2}{16} - 4y\frac{b^3}{64} + \frac{b^4}{256} \\
+ b\left(\cancel{y^3} - 3y^2\frac{b}{4} + 3y\frac{b^2}{16} - \frac{b^3}{64}\right) \\
+ c\left(y^2 - 2y\frac{b}{4} + \frac{b^2}{16}\right) \\
+ d\left(y - \frac{b}{4}\right) \\
+ e = 0
\end{aligned}$$

The equation now has the form,

$$y^4 + py^2 + qy + r = 0$$

where we can easily express p, q, r in terms of b, c, d, e from the above "pyramid",

$$\begin{aligned} p &= \frac{6b^2}{16} - \frac{3b^2}{4} + c, \\ q &= -\frac{4b^3}{64} + \frac{3b^3}{16} - \frac{2bc}{4} + d, \\ r &= \frac{b^4}{256} - \frac{b^4}{64} + \frac{b^2c}{16} - \frac{bd}{4} + e. \end{aligned}$$

We leave only the term in y^4 on the left side, giving,

$$y^4 = -py^2 - qy - r$$

and complete the square on it by adding $u^2y^2 + \frac{u^4}{4}$ to both sides,

$$\begin{aligned} y^4 + u^2y^2 + \frac{u^4}{4} &= u^2y^2 + \frac{u^4}{4} - py^2 - qy - r \\ \left(y^2 + \frac{u^2}{2}\right)^2 &= \left(u^2 - p\right)y^2 - qy + \left(\frac{u^4}{4} - r\right) \end{aligned}$$

Now the right side must also be a perfect square so its discriminant $B^2 - 4AC = 0$, that is,

$$q^2 - 4\left(u^2 - p\right)\left(\frac{u^4}{4} - r\right) = 0 \Rightarrow u^6 - pu^4 - 4ru^2 + 4pr - q^2 = 0$$

If we put $z = u^2$, we have a cubic,

$$z^3 - pz^2 - 4rz + 4pr - q^2 = 0$$

We solve the cubic and obtain a real root α which we put equal to u^2. Then, returning to,

$$\left(y^2 + \frac{u^2}{2}\right)^2 = \left(u^2 - p\right)y^2 - qy + \left(\frac{u^4}{4} - r\right)$$

the right side is now a perfect square, so by the quadratic formula[4] it factors as,

$$\left(y - \frac{q + \Delta}{2(u^2 - p)}\right)\left(y - \frac{q - \Delta}{2(u^2 - p)}\right) \text{ where } \Delta = \sqrt{B^2 - 4AC}.$$

[4]Note $ax^2 + bx + c = 0 \Rightarrow x = \frac{-b \pm \Delta}{2a}$, $\Delta = \sqrt{b^2 - 4ac}$ which means we can factor $f(x) = ax^2 + bx + c = a(x + \frac{b + \Delta}{2a})(x + \frac{b - \Delta}{2a})$.

But since for a perfect square $\Delta = 0$, if $u^2 = \alpha$, this gives,

$$\left(y^2 + \frac{\alpha}{2}\right)^2 = \left(y - \frac{q}{2(\alpha - p)}\right)^2$$

We solve the two quadratics given by,

$$y^2 + \frac{\alpha}{2} = \pm\left(y - \frac{q}{2(\alpha - p)}\right)$$

to find the four roots of the quartic equation.

Example 5. *Solve* $y^4 - 5y - 6 = 0$
Solution
The equation already has the form $y^4 + py^2 + qy + r = 0$ *where* $p = 0,\ q = -5,\ r = -6$. *The auxiliary cubic* $z^3 - pz^2 - 4rz + 4pr - q^2 = 0$ *becomes,*

$$z^3 + 24z - 25 = 0$$

By the factor theorem, $\alpha = 1$ *is a root since* $1^3 + 24 \times 1 - 25 = 0$ *so we need to solve,*

$$\left(y^2 + \frac{\alpha}{2}\right) = \pm\left(y - \frac{q}{2(\alpha - p)}\right)$$
$$\Rightarrow y^2 + \frac{1}{2} = y + \frac{5}{2} \text{ and } y^2 + \frac{1}{2} = -y - \frac{5}{2}$$
$$\Rightarrow y^2 - y - 2 = 0 \text{ and } y^2 + y + 3 = 0$$
$$\Rightarrow y = -1,\ 2,\ \frac{-1 \pm \sqrt{-11}}{2} \qquad \diamond$$

1.5 Looking Ahead

We have derived formulas for the roots or zeros of polynomial equations of degree ≤ 4. In each case the zeros were expressed in terms of the coefficients of the polynomial using only the usual algebraic operations $(+, -, \times, \div)$ and the radicals (square roots, cube roots, etc.) and exponents $(x^2, \ldots)$ and which also involved the n^{th} roots of unity where the degree of the polynomial is n, and as we saw in the case of $n = 4$, also the k^{th} roots of unity where $k|n$. (In the solution of degree 4 polynomials we reached square roots). We say polynomials of degree ≤ 4 are solvable by radicals, whether real or complex.

Our goal is to prove that there are polynomials of degree ≥ 5 whose zeros cannot be expressed in such terms. In other words, there is no formula that can be used to find the roots of all polynomials of degree ≥ 5. Obviously, an infinite number of polynomials of any degree can be solved since, for degree 5 for example, we can form as many polynomials of the type,

$$f(x) = (x - a)(x - b)(x - c)(x - d)(x - e)$$

as we choose, and their roots are simply a, b, c, d, e.

Also, using the formulas above, we can solve any degree 5 polynomial which is the product of a linear polynomial and a degree 4 polynomial, or the product of a degree 3 polynomial and a degree 2 polynomial and so on. But unlike the cases of the polynomials of degree less than 5, there is no formula for finding the roots of all degree 5 and higher polynomials.

We want to prove the insolubility of the quintic and higher degree polynomials by radicals, that is, we cannot solve all polynomials of degree 5 (and above) by expressing the zeros in terms of the basic operations, extracting n^{th} roots and raising numbers to a power.

This is an extremely difficult problem, exacerbated historically by the facts that Evariste Galois, who gave us the theory essential to the solution of the problem,

- Died in a duel at age 20, due to either "femme fatale" or "vive la révolution," who knows?
- But in any case left a treatise of his ideas written the night before he died that other leading mathematicians either lost or, for many years, could not understand.

Briefly expressed, Galois proved a SEPARABLE[5] polynomial is solvable by radicals if its GALOIS GROUP is a SOLVABLE GROUP. Since the SYMMETRIC GROUPS, S_n, are not solvable for $n \geq 5$, polynomials of degree 5 or greater with Galois group ISOMORPHIC to S_n are not solvable by radicals.

The genius of Galois was to link GROUP THEORY to FIELD THEORY and specifically to FIELD EXTENSIONS built from the zeros of the polynomial under study.

We start with group theory, in particular the study of the symmetric groups S_n whose elements are the functions which permute or rearrange the set of numbers $\{1, 2, \ldots, n\}$.

[5]The upper case words signal what is to come, you do not need to understand them at this time.

Chapter 2

Group Theory Part I

Groups, Subgroups, Cyclic Subgroups

2.1 Groups

A group is an abstract mathematical object. Its inspiration is an abstraction from the axioms of integers, fractions, real and complex numbers. Each of these is a set and the binary arithmetic operations apply to each. A group requires a set and one binary operation, generally regarded as either addition or multiplication.

Definition 5. *group and group axioms*
In abstract terms we define a group as a set G together with a binary operation $*$, written $(G, *)$, such that the following axioms, taken from $\{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$, are satisfied:

1. *Closure law: For all $a, b \in G$, we have $a * b \in G$, that is, the result of a binary operation acting on any two elements of the group is another element of the group. We say the group is closed under $*$.*
2. *Associative law: For all $a, b, c \in G$ we have $a * (b * c) = (a * b) * c$*
3. *Identity law: There is an identity element $e \in G$ such that for all $a \in G$ we have $a * e = e * a = a$*
4. *Inverses law: For all $a \in G$ there is an element $b \in G$ such that $a * b = b * a = e$ and we write this b as a^{-1}.*

Example 6. *For an example of each axiom, when applied to $(\mathbb{Z}, +)$ we have statements such as,*

1. *Closure: $5, 7 \in \mathbb{Z}$ and $5 + 7 = 12 \in \mathbb{Z}$*
2. *Associativity: $2 + (3 + 4) = (2 + 3) + 4$*
3. *Identity: $e = 0$ since $3 + 0 = 0 + 3 = 3$*

4. *Inverses:* -3 *is the inverse of* 3 *since* $3+(-3)=(-3)+3=0$ *or, more commonly* $3-3=0$ $\diamond$

Definition 6. *commutative or abelian group*
If a group $(G,*)$ *satisfies* $a*b=b*a$ *for all* $a,b\in G$ *we say the group is commutative or abelian (after Niels Abel, the Norwegian algebraicist).*

Clearly, $(\mathbb{Z},+)$ is abelian. All of our number sets so far are abelian but, if you have studied matrices, matrix multiplication is not abelian.

Note 1. *Note that a group obeys the cancellation law* $a*b=a*c\Rightarrow b=c$ *since,*

$$\begin{aligned} a*b=a*c &\Rightarrow a^{-1}*(a*b)=a^{-1}*(a*c)\\ &\Rightarrow (a^{-1}*a)*b=(a^{-1}*a)*c\\ &\Rightarrow e*b=e*c\\ &\Rightarrow b=c \end{aligned}$$

where we used the inverse, associative and identity axioms of groups.

For the sake of simplicity we refer to a group $(G,*)$ as just G since the binary operation is mostly specified elsewhere. Along these lines we then drop the use of $*$ and just say statements like $a(bc)=(ab)c$ which can be understood to mean $a\times(b\times c)=(a\times b)\times c$ if the operation is multiplication or $a+(b+c)=(a+b)+c$ if the operation is ordinary addition. But we will find there are other binary operations besides the arithmetic ones.

Further, for inverses, a^{-1} suits multiplication, giving the usual $aa^{-1}=a/a=1$ but it means $-a$ when we are dealing with addition, thus $a+(-a)=0$, and of course we generally drop the parentheses and write $a-a=0$. The inverse elements for the arithmetic operations are 0 for addition and 1 for multiplication and we call -6 the additive inverse of 6 and $\dfrac{1}{6}$ the multiplicative inverse of 6.

$\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$ are obviously all groups under the operation of addition. The only group axiom that causes an issue with the sets $\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$ under the operation of multiplication is the inverse law and the existence of multiplicative inverses. No integer greater than 1 has a multiplicative inverse that is also an integer, for example, $1/7$ is the multiplicative inverse of 7 but $1/7\notin\mathbb{Z}$, failing closure, so $(\mathbb{Z},\times)$ is not a group.

As for $\mathbb{Q},\mathbb{R},\mathbb{C}$, the element 0 does not have a multiplicative inverse, that is there is no element b such that $0\times b=1$. But we can still form groups simply by deleting the element 0. So we have the multiplicative groups $\mathbb{Q}^\times,\mathbb{R}^\times,\mathbb{C}^\times$ where the exponent $\times$ means the zero element has been removed. Thus, for example, $\mathbb{C}^\times=\mathbb{C}-\{0\}$ or $\mathbb{C}/\{0\}$.

So we have four additive groups, $\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$, and three multiplicative groups $\mathbb{Q}^\times,\mathbb{R}^\times,\mathbb{C}^\times$. They are all infinite in size and they form the "inspiration" for an infinity of other groups, some finite, some infinite. If you know about matrices, an example of a different infinite group is the set of all 2×2 matrices under matrix addition. We

can also have them as a group under matrix multiplication but again we have an issue with inverses and we need to delete all matrices of the form,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad ad - bc = 0$$

2.2 Congruence

Definition 7. *congruence*
Let m be a positive integer. If m divides the difference $a - b$ of two integers a, b, we say "a is congruent to b modulo m" and write $a \equiv b (\mathrm{mod}\ m)$.

This means an expression such as $27 \equiv x (\mathrm{mod}\ 6)$ can have an infinite number of solutions or congruences, for example,

$$27 \equiv 15 (\mathrm{mod}\ 6)$$
$$27 \equiv -21 (\mathrm{mod}\ 6)$$
$$27 \equiv 123 (\mathrm{mod}\ 6)$$

Unless otherwise specified, we will always take the least positive result, namely, $27 \equiv 3\ (\mathrm{mod}\ 6)$. In simple terms, we can now say $p (\mathrm{mod}\ m)$ is the smallest positive remainder when p is divided by m. For example, $11 (\mathrm{mod}\ 3) \equiv 2$.

2.3 Finite Groups

2.3.1 Groups using Congruences

Let's now define a group that proves to be extremely useful.

Definition 8. *$\mathbb{Z}_n$ under addition modulo n*
$\mathbb{Z}_n$ is the set of all possible smallest positive remainders when the integers are divided by n. That is,

$$\mathbb{Z}_n = \{0, 1, 2, ..., n - 1\}$$

In words, $\mathbb{Z}_n$ is the set of all integers modulo n where we note that when an integer is divided by n, no remainder can be greater than $n - 1$.

Example 7. *For example, $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ with operation modulo 5, meaning any integer is replaced by its least positive remainder when divided by 5. Thus,*

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, ...$$

becomes,

$$0, 1, 2, 3, 4, 0, 1, 2, 3, 4, 0, 1, ...$$

leaving only the elements $0, 1, 2, 3, 4$.
If we set up what we can call an operations table for all possible combinations of the elements of $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ *under addition modulo 5, we have,*

Mod 5	*0*	*1*	*2*	*3*	*4*
0	*0*	*1*	*2*	*3*	*4*
1	*1*	*2*	*3*	*4*	*0*
2	*2*	*3*	*4*	*0*	*1*
3	*3*	*4*	*0*	*1*	*2*
4	*4*	*0*	*1*	*2*	*3*

where we used $4 + 4 = 8 \equiv 3 (\text{mod } 5)$ *etc.*

You can easily see the set $\mathbb{Z}_5$ *is closed under addition modulo 5, meaning only its elements* $0, 1, 2, 3, 4$ *are found in the table, that the associative law holds, that there is an identity 0 (e.g.,* $0 + 3 = 3$ *) and that every element has an additive inverse, the pairs being* $(0, 0), (1, 4), (2, 3)$. ◇

Since we can specify any positive integer n for $\mathbb{Z}_n$, we already have an infinite number of finite groups once we prove the next theorem, that the set $\mathbb{Z}_n$ together with the operation of addition modulo n is a group.

Theorem 1. *
The set $\mathbb{Z}_n$ *together with the operation of addition modulo* n *is a group.*

Proof. We need to prove the four group axioms in Definition 5 on page 25 hold.

1. Closure, that is, if $a, b \in \mathbb{Z}_n$ so does $a+b(\text{mod } n)$, that is $a+b \equiv c(\text{mod } n)$ where $c < n$.
   This is so since a, b are less than n, so either $a + b = c < n$ and we are done, or $a + b = n + c$ where we must have $c < n$, and therefore n divides the difference $a + b - c$ so by Definition 7, page 27, $a + b \equiv c (\text{mod } n)$.

2. Associative Law, that is if $a, b, c \in \mathbb{Z}_n$ then $a + (b + c) = (a + b) + c$. This is true since a, b, c are also integers.

3. Identity element is 0.

4. Inverse Law. Given $a \in \mathbb{Z}_n,\ 0 \leq a \leq n - 1$, then $(n - a) + a = 0$ making $n - a$ the inverse of a.

Hence $\mathbb{Z}_n$ is a group. □

2.3.2 Groups formed by the roots of polynomials

We will be concerned with the roots of polynomials. Let's consider two examples.

Example 8. *The roots of* $f(x) = x^3 - 1$ *form a group under complex multiplication. Since* $x^3-1 = (x-1)(x^2+x+1)$*, applying the quadratic formula to the second factor, the roots are* $1, \omega, \omega^2$ *where* $\omega = \dfrac{-1+\sqrt{3}i}{2}$*. We can check that* ω^2 *is the complex conjugate of* ω *since,*

$$\left(\frac{-1+\sqrt{3}i}{2}\right) \times \left(\frac{-1+\sqrt{3}i}{2}\right) = \left(\frac{-1-\sqrt{3}i}{2}\right)$$

The multiplication table shows $\{1, \omega, \omega^2\}$ *obeys the four group requirements. Note,* $\omega^3 = 1$ *and* $w^4 = w$*.*

$\times$	*1*	ω	ω^2
1	*1*	ω	ω^2
ω	ω	ω^2	*1*
ω^2	ω^2	*1*	ω

Example 9. *The roots of* $x^4 - 1 = (x^2-1)(x^2+1)$ *are* $\pm 1, \pm i$ *with multiplication table,*

$\times$	*1*	*-1*	i	$-i$
1	*1*	*-1*	i	$-i$
-1	*-1*	*1*	$-i$	i
i	i	$-i$	*-1*	*1*
$-i$	$-i$	i	*1*	*-1*

The multiplication table shows all four group axioms are satisfied. ◇

2.3.3 Subgroups

Definition 9. *subgroup*
Given a group $(G, *)$*, if* $H \subseteq G$ *(*H *is a subset of* G*) and* H *is also a group under the same operation* $*$ *as* G*, we say* H *is a subgroup of* G*.*

Notation 1. *If* H *is a subgroup of* G *we write* $H \leq G$*.*

Definition 10. *proper subgroup*
H *is a proper subgroup of* G *if it is a subgroup that does not contain all the elements of* G*, that is, as a set,* $H \subset G$ *but* $H \neq G$*. We write* $H < G$*.*

Example 10. $(\{0,2\}, \otimes) < (\mathbb{Z}_4, \otimes)$ *where* $\otimes$ *is addition modulo 4. The two tables show each is a group and that* $\{0,2\}$ *is a subset of* $\mathbb{Z}_4$*.*

$\mathbb{Z}_4$	0	1	2	3	$\{0,2\}$	0	2
0	0	1	2	3	0	0	2
1	1	2	3	0	2	2	0
2	2	3	0	1			
3	3	0	1	2			

We have two tests for subgroups. But first note that the next theorem is our first "if and only if" theorem. We need to prove a $P \Rightarrow Q$ statement and also the converse $Q \Rightarrow P$. So we first suppose $H < G$ and prove the three conditions and then conversely, if the three conditions are true, we prove $H > G$.

Theorem 2. ***
Let G be a group with identity element e and let H be a subset of G.
Then H is a subgroup of G if and only if the following conditions are true:

(i) $ab \in H$ *for all* $a, b \in H$.

(ii) $e \in H$.

(iii) $a^{-1} \in H$ *for all* $a \in H$.

Proof. First, suppose H is a subgroup of G.
Proof of (i).
Since, by the definition of a subgroup, H is a group with the same operation as G then the closure axiom for H says $ab \in H$ for all $a, b \in H$.
Proof of (ii).
Suppose f is the identity element for H. Then f is also an element of G since $H \subset G$. In H we have $ff = f$ and in G we have $fe = f$.
Then $ff = ef$ and by the cancellation law, $f = e$, making $e \in H$.
Proof of (iii).
Suppose $b \in H$ is the inverse of $a \in H$. Then $ab = e$. But in G, $aa^{-1} = e$ making $ab = aa^{-1}$. Then by the cancellation law, $b = a^{-1}$ or the inverse of every element in H is also in H. Put succinctly, $a^{-1} \in H$ for all $a \in H$.
Proof of the converse
Second, for the converse, we suppose H is a subset of G that satisfies the given conditions,

(i) $ab \in H$ for all $a, b \in H$.

(ii) $e \in H$.

(iii) $a^{-1} \in H$ for all $a \in H$.

We need to show the four group axioms apply. Closure is given by the first condition, the identity element by the second, inverses by the third and the associative law is obvious.
Hence $H < G$. □

Example 11. *A simple example of a subgroup of* $(\mathbb{Z}, +)$ *is* $(3\mathbb{Z}, +)$ *where* $3\mathbb{Z} = \{0, \pm 3, \pm 6, \pm 9, ...\} = \{3n \mid n \in \mathbb{Z}\}$. *Clearly,*

- $(3n) + (3m) = 3(n + m) \in 3\mathbb{Z}$ *for all* $3n, 3m \in 3\mathbb{Z}$.
- $0 \in 3\mathbb{Z}$
- $-3n \in 3\mathbb{Z}$ *for all* $3n \in 3\mathbb{Z}$

So the three conditions of Theorem 2 are satisfied.

In general, $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$. The proof is left to the reader.

A more convenient test for a subgroup is this Corollary to Theorem 2.

Corollary 3. *** (Subgroup Test)*
A nonempty subset H *of a group* G *is a subgroup of* G *if and only if for every* $a, b \in H$ *we have* $ab^{-1} \in H$.

Proof. First, assume H is a subgroup of G and $a, b \in H$. Then by Theorem 2's third condition, $b^{-1} \in H$, so $a, b^{-1} \in H$ and by the first condition, $ab^{-1} \in H$.

*****

Conversely, we assume if $a, b \in H$ then $ab^{-1} \in H$. Then H satisfies the group axioms since we have:

- Identity: Let $b = a$. Then by the assumption $aa^{-1} \in H$, but since $aa^{-1} = e$ in G we must have $e \in H$
- Inverses: Let $a = e$ in the assumption that $a, b \in H \Rightarrow ab^{-1} \in H$. Then for all $b \in H$, $eb^{-1} = b^{-1} \in H$.
- Closure: Put b^{-1} for b in the assumption. Note $(b^{-1})^{-1} = b$.
  Then $a(b^{-1})^{-1} = ab \in H$.
- Associativity in H follows from the fact that all the elements in H are also in G which is a group.

□

Example 12. *In the previous example, where* $3\mathbb{Z} \subset \mathbb{Z}$, *for every pair* $3m, 3n \in 3\mathbb{Z}$, *clearly so also does,*

$$3m - 3n = 3(n - m) \in 3\mathbb{Z}.$$

Therefore, under the operation of addition, $3\mathbb{Z}$ *is a subgroup of* $\mathbb{Z}$ ◇

Note 2. *Again let us note b^{-1} represents the inverse of b for any group operation. In the previous example we are dealing with addition, so $b^{-1} = -b$.*
Note also that $(b^{-1})^{-1} = b$ since, given the inverse of any element added to (or the relevant binary operation) the element is the identity, then we have both $b * b^{-1} = e$ and $b^{-1} * (b^{-1})^{-1} = e$, so $b * b^{-1} = b^{-1} * (b^{-1})^{-1}$ and by cancellation, $(b^{-1})^{-1} = b$.
Note further that $(ab)^{-1} = b^{-1}a^{-1}$ since,

$$(ab)(ab)^{-1} = e \text{ and } (ab)(b^{-1}a^{-1}) = abb^{-1}a^{-1} = aea^{-1} = aa^{-1} = e.$$

Hence, $(ab)(ab)^{-1} = (ab)(b^{-1}a^{-1})$ and by cancellation, $(ab)^{-1} = b^{-1}a^{-1}$.

2.3.4 Cyclic Subgroups

A cyclic subgroup is a group that can be generated by one of its elements meaning every element in the group can be formed from that one element by repeated applications of the binary operation. Symbolically we use only addition and multiplication, but the binary operations take many other forms.

Definition 11. *cyclic group*[1]
We define the cyclic group $< a >$ generated by the element a in the group G as,

- *for multiplication, $< a >= \{x \in G \mid x = a^n \text{ for some } n \in \mathbb{Z}\}$.*
- *for addition, $< a >= \{x \in G \mid x = \underbrace{a + a + \cdots + a}_{n} = na \text{ for some } n \in \mathbb{Z}.\}$*

Example 13. *For example, $(\mathbb{Z}_5, \text{addition modulo } 5)$ is a finite cyclic group generated by 2 since,*

$$\begin{aligned} &2 = 2, \\ &2 + 2 = 4, \\ &2 + 2 + 2 = 1, \\ &2 + 2 + 2 + 2 = 3, \\ &2 + 2 + 2 + 2 + 2 = 0 \end{aligned}$$

are all elements of $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.
Note any further addition of 2's always yields one of these five elements, for example $102 \times 2 \equiv 4 \pmod 5$. ◇

In general the group $(\mathbb{Z}_n, \text{ modulo } n) = \{0, 1, 2, \cdots, n-1\}$ is obviously cyclic by definition. It can be generated by any element a provided $gcd(a, n) = 1$.
(Try $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$ with $a = 3, 4$.)

The simplest example of an infinite cyclic group is $\mathbb{Z}$ which is generated by 1 since $n \times 1, n \in \mathbb{Z}$ gives us all the integers. We could also use -1.

[1] We prove $< a >$ is a group in Theorem 4, part (1)

Before we prove the theorem relating cyclic groups and subgroups, let us note that the word "order" is used in two different ways when we are dealing with elements and groups.

Definition 12. *order of a group*
The order of a group G is the number of elements in the group. We use $|G|$ as the symbol for the order of a group.

Example 14. $|\mathbb{Z}_5| = |\{0, 1, 2, 3, 4\}| = 5$
The order of $\mathbb{Q}$ is infinite. $\diamond$

Definition 13. *order of a group element*
Let G be a group with identity e and let $a \in G$. If there is a positive integer n such that $a^n = e$, then a is said to have finite order. The smallest such positive integer is called the order of a, written $|a|$.

Example 15. $2 \in \mathbb{Z}_5$ *and* $|2| = 4$ *since* $2^4 \equiv 1 \pmod 5$.

This is where the word cyclic comes from for finite groups. If $a^n = e$ then, under repeated multiplication by a, we have the cyclic group $< a >$ with elements,

$$< a >= \{e, a, a^2, \cdots, a^{n-1}, e, a, \cdots\} = \{e, a, a^2, \cdots, a^{n-1}\}$$

Think of this like a clock reducing any number of hours to 1 to 12. Clearly, the number of elements in $< a >$ is n and we have $| < a > | = |a| = n$.

We then prove the four parts of Theorem 4 relating cyclic groups and subgroups, specifically,

Theorem 4. ***
(1) The cyclic group $< a >= \{x \in G \mid x = a^k \text{ for some } k \in \mathbb{Z}\}$ is a subgroup of G, the operation being multiplication.
(2) If $|a| = n$ then the cyclic subgroup $< a >$ is a finite group given by

$$< a >= \{e, a, a^2, \cdots, a^{n-1}\},$$

and therefore $| < a > | = n = |a|$.
(3) A finite group G is cyclic if and only if there exists an element $a \in G$ such that the order of G equals the order of a, that is, $|a| = |G|$.
(4) A finite cyclic group is abelian.

Proof. Proof of (1)
To show $< a >$ is a group, we use the criteria for a group from Definition 12.

- $< a >= \{x \in G \mid x = a^k \text{ for some } k \in \mathbb{Z}\}$ is closed since if $a^i, a^j \in < a >$ then $a^i a^j = a^{i+j} \in < a >$ since $i + j \in \mathbb{Z}$.
- Associativity follows from $a^i \times (a^j \times a^k) = (a^i \times a^j) \times a^k = a^{i+j+k}$.

- The identity element is $e = a^0 = 1$ since $a^0 \times a^k = a^k$. Note also $a^n = 1$, so $e = a^0 = a^n = 1$.
- Inverses exist since $(a^n)^{-1} = a^{-n}$ and $-n \in \mathbb{Z}$ so that $a^n(a^n)^{-1} = a^0 = 1$.

Alternatively, using Corollary 3, page 31, choose any $a^i, a^j \in < a >$.
Then $(a^j)^{-1} = a^{-j}$ and $a^i a^{-j} = a^{i-j} \in < a >$.
Either way, $< a >$ is a subgroup of G.
Proof of (2)
Given $|a| = n$ we can write any integer k divided by n as $k = qn + r, 0 \le r \le n-1$. Then,

$$a^k = a^{qn+r} = (a^n)^q a^r = e^q \times a^r = a^r, \ 0 \le r \le n-1.$$

Thus, all the integer powers, a^k, separate out into just the n elements a^r with powers $0 \le r \le n-1$. So,

$$< a >= \{e, a, a^2, \cdots, a^{n-1}\},$$

and therefore $| < a > | = n = |a|$.
Proof of (3)
Suppose G is cyclic. Then $G =< a >= \{e, a, a^2, \cdots, a^{n-1}\}$ and clearly $|a| = |G|$ since both equal n.

*****

Conversely, suppose $a \in G$ and $|a| = n = |G|$. Then $a^1, a^2, \cdots, a^n = e$ all belong to G and since $|G| = n$, there can be no other elements. Then, G is cyclic by (2).
Proof of (4)
Let $< g >= G$, that is g is a generator of the cyclic group G.
Let $a, b \in G$. Then $a = g^x, b = g^y$ for some $x, y \in \mathbb{Z}$ which is abelian.
Since,

$$ab = g^x g^y = g^{x+y} = g^{y+x} = g^y g^x = ba$$

then G is abelian. □

Note 3. *Part (3) of Theorem 4 has given us an easy test for a finite group to be cyclic, namely, a group G is cyclic if and only if it contains an element a of order $|G|$, that is, $a^n = 1$ where n is the number of elements in the group G or $n = |G|$.*

Chapter 3

Group Theory Part II

Symmetric Groups

3.1 Relations and Functions

We first need to recall some algebraic facts concerning relations and functions.

Definition 14. *relation*
A relation is a set of ordered pairs (x, y) of elements, the first element taken from a set called the domain, the second from a set called the range. We often use A, B for the two sets.

Example 16. *$\{(1,2),(5,6),(1,-7)\}$ is a relation on $\mathbb{Z}$.*
The domain is the set $A = \{1, 5, -1\}$, the range is the set $B = \{2, 6, -7\}$. ◇

Definition 15. *function*
Given sets A and B, a function f from A to B is a rule that assigns to each $x \in A$ exactly one element $y \in B$. We write $f(x) = y$ to illustrate that f assigns x to y. It is spoken as "f of x equals y."

Accordingly, we say a function f is a rule that maps elements of a set A (the domain) onto elements of a second set B (the range) such that for any $x \in A$ there is only one $y \in B$. Symbolically, we have,

$$f : A \to B$$

spoken as "f maps the set A onto the set B." We always need to specify what the rule f is as in the following example.

Example 17. *$f : \mathbb{Z} \to \mathbb{Q}, f(x) = \dfrac{6 - 2x}{3}$ is a function since any value of x gives only one possible result.*
For example if $x = 7$ then the unique result is $f(7) = \dfrac{6-14}{3} = \dfrac{-8}{3}$. Using $y = f(x)$, we

can also write this function as $2x + 3y = 6$ *where the rule is not explicit, we need to do a little algebra to find* $y = \dfrac{6-2x}{3} = f(x)$.
But $y^2 + 3x = 6$ *is not a function because you cannot solve for exactly one value of* y *since,*

$$y^2 + 3x = 6 \Rightarrow y^2 = 6 - 3x \Rightarrow y = \pm\sqrt{6-3x}$$

Thus if, say, $x = 1$, *there are the two* $y-$*values,* $\pm\sqrt{3}$. ◇

3.2 One-to-one and Onto Functions

We mostly need our functions to be more tightly defined than just if $f : A \to B$ is a function then for each $x \in A$ there is exactly one $y \in B$ such that $f(x) = y$. We often want the two sets to mirror one another exactly. We begin with the definitions that allow us to tighten up our concept of more useful functions.

Definition 16. *one-to-one function*
$f : A \to B$ *is a one-to-one function if for all* $x, y \in A$ *the equality* $f(x) = f(y)$ *means we must have* $x = y$.

Example 18. *The function* $f : \mathbb{Z} \to \mathbb{Z}, f(x) = x^3 + 1$ *is one-to-one since,*

$$f(x) = f(y) \Rightarrow x^3 + 1 = y^3 + 1 \Rightarrow x^3 = y^3 \Rightarrow x = y$$

The function $f : \mathbb{Z} \to \mathbb{Z}, f(x) = x^2 + 1$ *is not one-to-one since,*

$$f(3) = f(-3) = 10 \text{ but } 3 \neq -3.$$ ◇

Definition 17. *onto function*
$f : A \to B$ *is onto if for all* $b \in B$ *there is an* $a \in A$ *such that* $b = f(a)$.

Example 19. $f : \mathbb{R} \to \mathbb{R}, f(x) = x^3 + 1$ *is onto since we can solve* $y = x^3 + 1$ *for* x *as* $x = \sqrt[3]{y-1}$ *thus ensuring every element* y *of the second* $\mathbb{R}$ *comes from an element* x *in the first* $\mathbb{R}$. *Thus* $y = 9$ *is the mapping of* $x = 2$.
However, $f : \mathbb{R} \to \mathbb{R}, f(x) = x^2$ *is not onto since all the negative numbers in the second* $\mathbb{R}$ *have not been produced by squaring the numbers in the first* $\mathbb{R}$. ◇

Definition 18. *one-to-one correspondence*
$f : A \to B$ *is a one-to-one correspondence if it is both one-to-one and onto*[1].

Note 4. *The simple way to remember the definition of a one-to-one correspondence between the elements of two finite sets is that it is a function where every element of one set is paired with exactly one element of the other set and every element of the other set is paired with exactly one element of the first set. We will formally prove this later but we will use it several times.*

[1] Due to the work of French mathematicians we also have the nomenclature of injective, surjective and bijective functions for one-to-one, onto and one-to-one correspondences respectively.

Another attribute we would like most of our functions to have is that they have an inverse. That is, given a function $f : A \to B$ we would like to have a function $g : B \to A$ such that if $f(x) = y$ then $g(y) = x$. We encountered this dualism in our college algebra course. Let's revisit it.

3.3 Composition of Functions and Inverse Functions

Definition 19. *composition of functions*
The composition of two functions f, g acting on the variable x is written $f \circ g(x)$ and is defined by,

$$f \circ g(x) = f(g(x))$$

In words we read $f \circ g(x)$ as "f of g(x)." Again, for brevity, if the context is clearly composition of functions, we abbreviate $f \circ g$ to fg.

Example 20. *If $f(x) = 3x - 1, g(x) = 6 - 5x$, then,*

$$\begin{aligned} f \circ g(x) &= f(g(x)) \\ &= 3g(x) - 1 \\ &= 3(6 - 5x) - 1 \\ &= -15x + 17 \end{aligned}$$

We prove the following about the composition of functions.

Theorem 5. ****
Let $f : A \to B, g : B \to C, h : C \to D$ be three maps. Then,

(1) Associativity: $h \circ (g \circ f) = (h \circ g) \circ f$

(2) If f and g are both one-to-one so is their composition $g \circ f$

(3) If f and g are both onto so is their composition $g \circ f$

Proof. We prove the three parts separately.

(1) For any $x \in A$ we have by Definition 19 on page 37 of composition of functions that,

$$h \circ (g \circ f)(x) = h(g \circ f)(x) = h(g(f(x))) = (h \circ g)(f(x)) = (h \circ g) \circ f(x)$$

(2) By Definition 16 on page 36 of a one-to-one function we need to prove that if $(g \circ f)(x) = (g \circ f)(y)$ then $x = y$.
Suppose f and g are both one-to-one and let $(g \circ f)(x) = (g \circ f)(y)$.
Then $g(f(x)) = g(f(y))$ and since g is one-to-one, we have $f(x) = f(y)$.
But f is also one-to-one so $x = y$, proving $g \circ f$ is also one-to-one.

(3) We have the two onto functions $f : A \to B$ and $g : B \to C$. By Definition 17 on page 36 of an onto function, we need to prove for all $z \in C$ that there is an $x \in A$ such that $(g \circ f)(x) = z$.
Let $z \in C$. Since $g : B \to C$ is onto, there must be some $y \in B$ such that $g(y) = z$. Then since $f : A \to B$ is onto, if $y \in B$ there must be some $x \in A$ such that $f(x) = y$.
That means $g(f(x)) = g(y) = z$, so we have found an element $x \in A$ with $g(f(x)) = z$. So $g \circ f$ is onto.

□

As we do in a college algebra course, let us now move on to inverse functions.

Definition 20. *inverse function*
A function f has an inverse function g if we have the two compositions,

$$f(g(x)) = x \text{ for all } x \text{ in the domain of } g.$$
$$g(f(x)) = x \text{ for all } x \text{ in the domain of } f.$$

Notation 2. *We use the symbol f^{-1} for the inverse function of the function f and have,*

$$f(f^{-1}(x)) = x, \quad f^{-1}(f(x)) = x.$$

Example 21. *The inverse function of $f(x) = 3x + 7$ is obtained as follows. Write $y = 3x + 7$ and then interchange x and y to obtain $x = 3y + 7$. Rearrange this to $y = \dfrac{x-7}{3}$ and we then have the inverse function $f^{-1}(x) = \dfrac{x-7}{3}$. We prove this is correct by forming,*

$$f \circ f^{-1}(x) = f(f^{-1}(x)) = 3f^{-1}(x) + 7 = 3 \times \frac{x-7}{3} + 7 = x$$

as required by the definition, and similarly we need to show $f^{-1}(f(x)) = x$. ◇

So we want our functions to be one-to-one correspondences and to have inverses. As we will see in Lemma 6, these are equivalent conditions, that is, a function is a one-to-one correspondence if and only if it has an inverse.

Lemma 6. *** The function $f : A \to B$ has an inverse if and only if it is a one-to-one correspondence.*

Proof. First, suppose that f has an inverse. We need to show f is one-to-one and onto.
To show f is onto[2] we need to show for all $y \in B$ there exists an $x \in A$ such that $f(x) = y$.

[2]Definition 17, page 36

If f has an inverse then let it be $g : B \to A$.
So, given any $y \in B$ let $x = g(y) \in A$.
Now by Definition 20 on page 38 of inverse functions, $f(g(y)) = y$. Then $f(x) = y$ so f is onto since for all $y \in B$ there exists an $x \in A$ such that $f(x) = y$.

**

To show f is one-to-one[3] we need to show if $f(a) = f(b)$ then $a = b$.
If $f(a) = f(b)$ for some $a, b \in A$, then (applying g to both sides) $g(f(a)) = g(f(b))$.
But by Definition 20 on page 38 of inverse functions, $g(f(a)) = a$ and $g(f(b)) = b$ so $a = b$. Thus, f is one-to-one.
So f is both onto and one-to-one and therefore a one-to-one correspondence and we have proved the first part of the theorem.

*****

Conversely, suppose that f is a one-to-one correspondence. We want to show f has an inverse g such that $f(g(x)) = x$ and $g(f(x)) = x$.
Given $x \in B$, there exists a $y \in A$ with $f(y) = x$ (since f is onto).
Moreover, there is only one such y, since if we also have $f(z) = x$ then since f is one-to-one, we have $f(z) = f(y) \Rightarrow z = y$.
Define $g(x)$ to be equal to this y.
Then if $g(x) = y$ and $x = f(y)$ then $g(f(y)) = y$ for any y and also if $f(y) = x$ and $y = g(x)$ then $f(g(x)) = x$ for any x and so by definition, g is the inverse[4] of f.
This completes the proof of the second part of the theorem. □

3.4 Symmetric Groups

The most important groups required to prove the insolvability of the quintic and all polynomials of degree ≥ 5 are the symmetric groups.

Definition 21. *symmetric groups*
We define the n^{th} symmetric group S_n as the set of all permutations or rearrangements of the numbers $1, 2, 3, \cdots, n$.

Example 22. *For example, S_3 is the set of six permutations of the numbers 1,2,3. We label the permutations ϕ_0, $\phi_1, \cdots, \phi_5$. They act on $1, 2, 3$ and, except for the identity permutation, ϕ_0, create different arrangements thus,*

$$\phi_0 : 1,2,3 \to 1,2,3 \qquad \phi_1 : 1,2,3 \to 1,3,2$$
$$\phi_2 : 1,2,3 \to 2,1,3 \qquad \phi_3 : 1,2,3 \to 2,3,1$$
$$\phi_4 : 1,2,3 \to 3,1,2 \qquad \phi_5 : 1,2,3 \to 3,2,1$$

[3]Definition 16, page 36
[4]Definition 20, page 38

So we describe the permutations themselves as functions that act on the elements of $\{1,2,3\}$ *and we say* $S_3 = \{\phi \mid \phi$ *permutes* $1,2,3\}$ *where each of the six* ϕ_i *functions acts on the elements* $1,2,3$ *and rearranges them into one of the six possible permutations. Note a permutation* ϕ_i *is obviously a one-to-one correspondence since every element of the first set is clearly paired with just one element of the second set and vice versa. Accordingly we can write* $S_3 = \{\phi_0, \phi_1, \phi_2, \phi_3, \phi_4, \phi_5\}$ *where* ϕ_1 *for example acts on the top line of* $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$*, creating the rearrangement on the bottom line as follows,*

$$\begin{aligned} \phi_1(1) &= 1 \\ \phi_1(2) &= 3 \\ \phi_1(3) &= 2 \end{aligned}$$

Similarly ϕ_2 *creates* $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ *and so on except for* ϕ_0 *which is the identity permutation function creating* $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ *by leaving the elements unchanged.* ◇

We prove in Theorem 7 that in general S_n has $n!$ possible permutations of the set $A = \{1,2,\cdots,n\}$ or $|S_n| = n!$

Theorem 7. ***
There are $n!$ *possible permutations of the set* $A = \{1,2,\cdots,n\}$ *or* $|S_n| = n!$

Proof. Let $\phi \in S_n$. Then ϕ can be written as,

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ \phi(1) & \phi(2) & \phi(3) & \ldots & \phi(n-1) & \phi(n) \end{pmatrix}$$

There are n choices for $\phi(1)$ and $n-1$ choices for $\phi(2)$, etc. Therefore the total number of choices is $n(n-1)(n-2)\cdots 1 = n!$ □

3.5 Notations for Permutations

3.5.1 First Notation

We adopt several notations for permutations. For example, for S_5 (which has $5! = 120$ permutations) we can write one of the permutations as,

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{pmatrix}$$

meaning, as above, that ϕ is the permutation function which acts on 1 2 3 4 5 according to,

$$\phi(1) = 3, \phi(2) = 1, \phi(3) = 4, \phi(4) = 5, \phi(5) = 2$$

3.5.2 Second Notation

But we can also write $\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{pmatrix}$ as a cycle read from left to right and looping back to the beginning, namely, $\phi = (1\ 3\ 4\ 5\ 2)$, meaning ϕ sends,

$$1 \to 3, 3 \to 4, 4 \to 5, 5 \to 2, 2 \to 1$$

As will become clear when we review multiplication of cycles below, in this notation the identity element of S_n is $(1)(2)\dots(n)$.

Example 23. *In cycle notation,* $S_3 = \{(1,2,3), (1,3,2), (2,3), (1,3), (1,2), (1)(2)(3)\}$ *The two notations relate as follows.*

$$\sigma_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = (1)(2)(3) \text{ or } \{\ \} \qquad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (23)$$

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123) \qquad \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (13)$$

$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132) \qquad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (12)$$

Note if we follow the practice of omitting 1-cycles then the identity $(1)(2)(3)$ *is simply written as* $\{\ \}$.

3.5.3 Third Notation

Finally, we can often write ϕ as a product of cycles, for example $\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$ consists of two separate or disjoint cycles $1 \to 3 \to 1$ and then we start again with $2 \to 4 \to 5 \to 2$.
We can therefore write,

$$\phi = (1\ 3)(2\ 4\ 5)$$

In each case the cycle is closed once the beginning element is repeated. Note when the first cycle beginning with 1 is completed by looping back to the beginning, we start the next cycle with the next highest number not already taken care of in the first cycle (in this case 2) and so on if there are more than two cycles.

Note (1 3) only affects the numbers 1 and 3, the other numbers remain "fixed". Similarly (2 4 5) only affects the numbers $2, 4, 5$ with 1 and 3 being fixed.

Accordingly, to determine the meaning of $\phi = (1\ 3)(2\ 4\ 5)$ we start with the number 1 thus,

$$\phi(1) = (1\ 3)(2\ 4\ 5)(1)$$

and progress right to left first through $(2\ 4\ 5)$ and then through $(1\ 3)$ thus: $3 \leftarrow 1 \leftarrow 1$, giving, $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & & & & \end{pmatrix}$ Similarly, we have,

$$\begin{aligned} 4 &\leftarrow 4 \leftarrow 2 \\ 1 &\leftarrow 3 \leftarrow 3 \\ 5 &\leftarrow 5 \leftarrow 2 \\ 2 &\leftarrow 2 \leftarrow 5, \end{aligned}$$

giving $\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 4 \end{pmatrix}$ as we require. Before we define cycle multiplication, let's take another example,

Example 24. *Consider the permutation,*

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 9 & 1 & 8 & 6 & 4 & 3 & 5 & 2 \end{pmatrix}$$

We can rearrange this permutation without altering any value of $\phi(a) = b$ as follows.

$$\phi = \begin{pmatrix} 1 & 7 & 3 & \mathbf{2} & \mathbf{9} & 4 & 8 & 5 & 6 \\ 7 & 3 & 1 & \mathbf{9} & \mathbf{2} & 8 & 5 & 6 & 4 \end{pmatrix}$$

In effect the permutation $\phi \in S_9$ partitions the set $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, \}$ into three disjoint pieces $(1, 7, 3), (2, 9,), (4, 8, 5, 6)$. ϕ moves around the elements in each piece but does not move elements between pieces.
Let us write the permutation that takes 1 to 7, 7 to 3 and 3 to 1 as (1 7 3), that is,

$$(1\ 7\ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 2 & 1 & 4 & 5 & 6 & 3 & 8 & 9 \end{pmatrix}$$

Note that all the elements other than 1,7,3 are "fixed", that is $\phi(4) = 4$, etc.
Similarly we can write $(2\ 9)$ and $(4\ 8\ 5\ 6)$ where,

$$(2\ 9) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 9 & 3 & 4 & 5 & 6 & 7 & 8 & 2 \end{pmatrix}$$

$$(4\ 8\ 5\ 6) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 2 & 3 & 8 & 6 & 4 & 7 & 5 & 9 \end{pmatrix}$$

Once we confirm how to multiply cycles, as we did above, we can easily show the original permutation,

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 9 & 1 & 8 & 6 & 4 & 3 & 5 & 2 \end{pmatrix}$$

is their product , that is,

$$\phi = (1\ 7\ 3)(2\ 9)(4\ 8\ 5\ 6) \qquad \diamond$$

3.6 Multiplication of two permutations in cycle format

In general, suppose we wish to find the composition of two permutations $\sigma,\ \tau$ given by,

$$\sigma\tau = (a_1, a_2, \cdots, a_k)(b_1, b_2, \cdots, b_m).$$

Start with 1 and work right to left.

- If 1 is the element b_j in τ we use $\tau(b_j) = b_{j+1}$ (or if $1 = b_m$ then $\tau(b_m) = b_1$).

  We then look for b_{j+1} in σ.

  - If we find $b_{j+1} = a_s$ then we use $\sigma(a_s) = a_{s+1}$. (or a_1 where $s = k$.) We conclude $\sigma\tau(1) = b_{j+1}$. (or a_1.)
  - If we find there is no $a_i = b_{j+1}$ then we conclude $\sigma\tau(1) = b_{j+1}$.

- If 1 is not an element in τ then τ leaves 1 fixed and we search for it in σ. If we find $1 = a_s$ then we use $\sigma(a_s) = a_{s+1}$ (or a_1 where $s = k$.) We conclude $\sigma\tau(1) = a_{s+1}$. (or a_1.)

- If 1 is not an element of either τ or σ then we conclude $\sigma\tau(1) = 1$, that is 1 is fixed.

So, if we want to write the product as a product of disjoint cycles, then start with 1 and find $\sigma\tau(1) = j$ say. Then repeat the process for j and if we find $\sigma\tau(j) = k$, then repeat the process for k until eventually we again reach 1 and that first cycle is complete. For the second cycle, choose the smallest number not in the first cycle and repeat the process until it is found again thus closing off the second cycle, and so on until all the elements in σ, τ have been allocated to a cycle.

Example 25. *Let us return to* $\phi = (173)(29)(4856)$. *We want to show*

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 9 & 1 & 8 & 6 & 4 & 3 & 5 & 2 \end{pmatrix}$$

Start with 1, that is, calculate $\phi(1) = (173)(29)(4856)(1)$
Working right to left, note (4856) does not change 1 and neither does (29) but (173) sends 1 to 7 so we have $7 \leftarrow 1 \leftarrow 1 \leftarrow 1$ *giving* $\phi = \begin{pmatrix} 1 & \\ 7 & \end{pmatrix}$
Next calculate $\phi(7)$. *We have* $3 \leftarrow 7 \leftarrow 7 \leftarrow 7$ *so* $\phi = \begin{pmatrix} 1 & 7 \\ 7 & 3 \end{pmatrix}$
Next $\phi(3)$ *gives* $1 \leftarrow 3 \leftarrow 3 \leftarrow 3$ *so* $\phi = \begin{pmatrix} 1 & 3 & 7 \\ 7 & 1 & 3 \end{pmatrix}$

Since we are back to 1, we choose the next highest number which is 2.

Then $\phi(2)$ *gives* $9 \leftarrow 9 \leftarrow 2 \leftarrow 2$ *so* $\phi = \begin{pmatrix} 1 & 2 & 3 & & 7 & \\ 7 & 9 & 1 & & 3 & \end{pmatrix}$

Then $\phi(9)$ *gives* $2 \leftarrow 2 \leftarrow 9 \leftarrow 9$ *so* $\phi = \begin{pmatrix} 1 & 2 & 3 & & 7 & 9 \\ 7 & 9 & 1 & & 3 & 2 \end{pmatrix}$

Since we are back to 2 we choose the next highest unused number, namely 4. The remaining products are,

$$8 \leftarrow 8 \leftarrow 8 \leftarrow 4$$
$$5 \leftarrow 5 \leftarrow 5 \leftarrow 8$$
$$6 \leftarrow 6 \leftarrow 6 \leftarrow 5$$
$$4 \leftarrow 4 \leftarrow 4 \leftarrow 6$$

So, $\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 9 & 1 & 8 & 6 & 4 & 3 & 5 & 2 \end{pmatrix}$ $\diamond$

We do not need to revert to the first notation to calculate cycle products as this next example demonstrates.

Example 26. *Calculate the product* $\sigma\tau$ *in cycle form where,*

$$\sigma = (16527348),\ \tau = (152468)(37).$$

Remember we work right to left beginning with the action on 1. Then,

$$\sigma \circ \tau = (16527348)(152468)(37)$$
$$2 \leftarrow 5 \leftarrow 1 \leftarrow 1$$
$$= (12$$
$$8 \leftarrow 4 \leftarrow 2 \leftarrow 2$$
$$= (128$$
$$6 \leftarrow 1 \leftarrow 8 \leftarrow 8$$
$$= (1286$$
$$1 \leftarrow 8 \leftarrow 6 \leftarrow 6$$
$$= (1286)(3$$
$$3 \leftarrow 7 \leftarrow 3$$
$$= (1286)(3)(4$$
$$5 \leftarrow 6 \leftarrow 4 \leftarrow 4$$
$$= (1286)(3)(45$$
$$7 \leftarrow 2 \leftarrow 5 \leftarrow 5$$
$$= (1286)(3)(457$$
$$4 \leftarrow 3 \leftarrow 3 \leftarrow 7$$
$$= (1286)(3)(457)$$

We usually omit single element cycles, thus,

$$\begin{aligned}\sigma \circ \tau &= (1286)(457) \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 8 & 3 & 5 & 7 & 1 & 4 & 6 \end{pmatrix}. \end{aligned} \qquad \diamond$$

3.7 More on cycles

Using the binary operation of composition of functions, that is, $\sigma \circ \tau(a) = \sigma(\tau(a))$, we prove in Theorem 8 that S_n is a group.

Theorem 8. ***
The set S_n of all permutations of the set $A = \{1, 2, \ldots, n\}$ is a group under permutation multiplication or composition of functions.

Proof. The four axioms for a group in Definition 5 on page 25 are satisfied, since,

1. (Closure) By definition, permutations are one-to-one and onto functions and permutation multiplication is simply composition of one-to-one correspondences. By Theorem 5 on page 37, the composition of two one-to-one correspondences is again a one-to-one correspondence (one-to-one and onto) so we have closure.

2. (Associativity) By Theorem 5 the composition of functions is associative.

3. (Identity) The identity is $\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots & n \\ 1 & 2 & 3 & 4 & \ldots & n \end{pmatrix}$

4. (Inverses) For example, if $\phi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ a & b & c & d \end{pmatrix}$ then we simply interchange the two rows and $\phi^{-1} = \begin{pmatrix} a & b & c & d \\ 1 & 2 & 3 & 4 \end{pmatrix}$ is the inverse function of ϕ such that,
$$\phi^{-1}\phi = \begin{pmatrix} a & b & c & d \\ 1 & 2 & 3 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ a & b & c & d \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

Hence S_n is a group under the operation of permutation multiplication. □

3.7.1 Inverses of permutations

We note the Inverses part of the proof of Theorem 8, namely, if $\phi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ a & b & c & d \end{pmatrix}$ then, interchanging the two rows, $\phi^{-1} = \begin{pmatrix} a & b & c & d \\ 1 & 2 & 3 & 4 \end{pmatrix}$ is the inverse function.
In practice we would rearrange the top row of ϕ^{-1} so that the elements on the top line are in numerical order, 1, 2, etc., as in the following example.

Example 27. *If* $\phi = \begin{pmatrix}1&2&3&4\\3&1&4&2\end{pmatrix}$ *then* $\phi^{-1} = \begin{pmatrix}3&1&4&2\\1&2&3&4\end{pmatrix} = \begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix}$
making, $\phi^{-1} \circ \phi = \begin{pmatrix}1&2&3&4\\3&1&4&2\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix} = \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$ ◇

Note 5. *In cycle notation, if* $\phi = (ab\ldots cd)$ *then* $\phi^{-1} = (dc\ldots ba)$*, the reversal of the elements of* ϕ*.*

Example 28. *For example, in* S_3*, the inverse of* (312) *is* (213) *since* $(312)(213) = (1)(2)(3)$. ◇

3.7.2 Composition of cycles is abelian or commutative

Theorem 9. ** *Let* $A = \{1, 2, \ldots, n\}$ *and* $\sigma, \tau \in S_n$ *be disjoint cycles. Then,*

$$\sigma\tau = \tau\sigma \text{ or } \sigma \circ \tau(x) = \tau \circ \sigma(x) \text{ for all } x \in A.$$

That is, the composition of disjoint cycles is abelian or it commutes.

Proof. Let $\sigma = (a_1, a_2, \ldots, a_m)$ *and* $\tau = (b_1, b_2, \ldots, b_n)$ where $a_i \neq b_j$ for all i, j such that $1 \leq i \leq m, 1 \leq j \leq n$, that is the cycles are disjoint.
Note τ leaves the elements a_i fixed (that is $\tau(a_i) = a_i$) and σ leaves the elements b_j fixed.
Then, using Definition 19 on page 37 of composition of functions, that is $\sigma \circ \tau(x) = \sigma(\tau(x))$, we have for $x = a_i$,

$$\sigma \circ \tau(a_i) = \sigma(\tau(a_i)) = \sigma(a_i) = a_{i+1} = \tau(a_{i+1}) = \tau(\sigma(a_i)) = \tau \circ \sigma(a_i),$$

unless $a_i = a_m$, in which case,

$$\sigma \circ \tau(a_m) = \sigma(\tau(a_m)) = \sigma(a_m) = a_1 = \tau(a_1) = \tau(\sigma(a_m)) = \tau\sigma(a_m)$$

A similar argument applies to $x = b_j$ and $\sigma\tau(b_j)$. Then $\sigma\tau = \tau\sigma$ for all the elements of σ and τ proves the composition of two disjoint cycles is abelian or it commutes. □

3.7.3 k-cycles and 2-cycles

Definition 22. *- k-cycles and 2-cycles*
We define a k-cycle as a cycle with k elements or length k. A 2-cycle has 2 elements or length 2.

We prove in Theorem 10 that every cycle of any length can be written as a product of 2- cycles.

Theorem 10. ****
Every cycle can be written as the product of 2-cycles, namely,

$$\phi = (a_n a_{n-1})(a_n a_{n-2}) \dots (a_n a_2)(a_n a_1)$$

Proof. Let $\phi = (a_1, a_2, \dots, a_n)$ and consider $(a_n a_{n-1})(a_n a_{n-2}) \dots (a_n a_2)(a_n a_1)$. Start with their action on a_1.

$$\begin{aligned}
&(a_n a_{n-1})(a_n a_{n-2}) \dots (a_n a_3)(a_n a_2)(a_n a_1)(a_1) \\
&\quad a_2 \leftarrow \dots \leftarrow a_2 \leftarrow a_n \leftarrow a_1 \\
&\quad = (a_1 a_2 \\
&\quad a_3 \leftarrow \dots \leftarrow a_3 \leftarrow a_n \leftarrow a_2 \\
&\quad = (a_1 a_2 a_3 \\
&\quad = \dots\dots \\
&\quad = (a_1 a_2 a_3 \dots a_n)
\end{aligned}$$

□

Example 29. *(24513) = (31)(35)(34)(32)*

Note 6. *The exposition $\phi = (a_n a_{n-1})(a_n a_{n-2}) \dots (a_n a_2)(a_n a_1)$ is not unique, for example, we can also have $\phi = (a_1 a_2)(a_1 a_3) \dots (a_1 a_{n-1})(a_1 a_n)$.*

3.8 The Alternating Subgroup

Definition 23. *even and odd permutations*
We label permutations as even and odd permutations, meaning the permutation is respectively either the product of an even number of 2−cycles or an odd number of 2−cycles. We label the set of even permutations as A_n.

We prove in general in Theorem 11 that A_n is a subgroup of S_n which we name the alternating group. We prove in Theorem 12 that exactly half the elements of S_n are even permutations and the other half are odd, so that $|A_n| = \dfrac{|S_n|}{2} = \dfrac{n!}{2}$.

Theorem 11. ***
The set of even permutations, A_n, is a subgroup of the symmetric group S_n.

Proof. Note the inverse of a 2-cycle is just its reverse, that is $(ab)^{-1} = (ba)$.
Let $\phi, \theta \in A_n$. By the subgroup test, Corollary 3 on page 31, we need to show $\phi\theta^{-1} \in A_n$. We have by definition that ϕ, θ are the product of an even number of 2-cycles, say,

$$\phi = \sigma_1 \sigma_2 \dots \sigma_{2n} \text{ and } \theta = \tau_1 \tau_2 \dots \tau_{2m}, \quad m, n \in \mathbb{N}.$$

But then,

$$\phi = \sigma_1\sigma_2\ldots\sigma_{2n} \text{ and } \theta^{-1} = (\tau_1\tau_2\ldots\tau_{2m})^{-1} = \tau_{2m}\tau_{2m-1}\ldots\tau_1,$$

are both the product of an even number of 2-cycles and therefore so is,

$$\phi\theta^{-1} = \sigma_1\sigma_2\ldots\sigma_{2n}\tau_{2m}\tau_{2m-1}\ldots\tau_1,$$

which has $(2n+2m)$ 2-cycles. So $\phi\theta^{-1} \in A_n$, proving A_n is a subgroup of S_n. □

Definition 24. *alternating subgroup*
The subset of even permutations in the symmetric group S_n is called the alternating subgroup for which we use the notation A_n.

Example 30. *Let us consider the $3! = 6$ permutations in S_n, the symmetric group of permutations on $A = \{1,2,3\}$. They are, using Theorem 16, page 53,*

$$\sigma_0 = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = (1)(2)(3) \qquad \sigma_3 = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = (23)$$
$$\sigma_1 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = (123) = (32)(31) \qquad \sigma_4 = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = (13)$$
$$\sigma_2 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = (132) = (23)(21) \qquad \sigma_5 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = (12)$$

Note the alternating group A_3 is a subgroup of S_3 as we proved in Theorem 17 above, and therefore must contain the identity σ_0.
Thus $A_3 = \{\sigma_0, \sigma_1, \sigma_2\} = \{(1)(2)(3), (32)(31), (23)(21)\}$.
You can show A_3 is closed by showing $\sigma_1^2 = \sigma_2$, $\sigma_2^2 = \sigma_1$ and $\sigma_1\sigma_2 = \sigma_0$. ◇

Theorem 12. ****
There are the same number of odd and even 2-cycles in S_n, that is the order of A_n is,

$$|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}.$$

Proof. Let $S_n = A_n \cup O_n$ where O_n is the set of odd permutations.
To show two sets have the same number of elements, we simply need to construct a one-to-one correspondence (one-to-one and onto function) between them since if such a function exists then each element in the first set corresponds to exactly one element in the second set and vice versa, so the two sets must have the same number of elements.
Let $\alpha : A_n \to O_n$ where for any $\sigma \in A_n$, $\alpha(\sigma) = \sigma(12)$, that is, an even permutation becomes an odd permutation by multiplying it by a 2-cycle (12).

First note that $\phi(12)(12) = \phi$ for any cycle ϕ since $(12)(12)$ is just the identity[5] as seen by their action on 1 and 2 and any other element.

$$(12)(12)(1) = 1,\ (12)(12)(2) = 2 \textit{ and } (12)(12)(a) = a \textit{ for all } a \neq 1, 2$$

Recall Definition 16 on page 36: For $\theta : A \to B$ to be one-to-one we need to show for all $x, y \in A$ that if $\theta(x) = \theta(y)$ then $x = y$.
Then α is one-to-one since if $\sigma, \tau \in A_n$, then,

$$\begin{aligned} &\alpha(\sigma) = \alpha(\tau) \\ &\Rightarrow \sigma(12) = \tau(12) \\ &\Rightarrow \sigma(12)(12) = \tau(12)(12) \\ &\Rightarrow \sigma = \tau \end{aligned}$$

Finally, for $\theta : A \to B$ to be onto, according to Definition 17 on page 36, we need to show for all $b \in B$ that there is an $a \in A$ such that $\theta(a) = b$.
Well then, $\alpha : A_n \to O_n$ is onto since if $\beta \in O_n$ is an odd permutation then $\beta(12)$ is an even permutation with,

$$\alpha(\beta(12) = \beta(12)(12) = \beta.$$

Simply expressed, for every $\beta \in O_n$ there is a $\beta(12) \in A_n$. Hence $\theta : A_n \to O_n$ is a one-to-one correspondence and $|A_n| = |O_n|$ so that $|A_n| = \dfrac{|S_n|}{2} = \dfrac{n!}{2}$ by Theorem 7 on page 40. □

It is this relationship between A_n and S_n that is critical to proving the insolvability by radicals of polynomials of degree ≥ 5.

3.9 Generators of S_n

In the conclusion of this book we will find an actual example of a non-solvable quintic by using Theorem 106, that an irreducible quintic with exactly three real roots (and two complex roots) is not solvable by radicals.

The proof of Theorem 106 requires Theorem 13 where we prove every permutation in S_n is a product of 2-cycles of the form $(i, i+1)$. We also need Theorem 14 where we prove that the cycles $(1, 2, \ldots, n)$ and (1,2) generate S_n, meaning every permutation in S_n can be formed by taking multiples of just $(1, 2, \ldots, n)$ and (1,2).

Theorem 13. *****
For $n \geq 2$, S_n is generated by the $(n-1)$ 2-cycles $(1,2), (2,3), \ldots, (n-1, n)$.

[5]Actually the product of any 2–cycle by itself is just the identity as you can easily see - try $(5,6)(5,6) \in S_6$.

Proof. We have already proved in Theorem 10 on page 47 that every cycle in S_n is the product of 2-cycles so it suffices to show any 2-cycle (a,b) in S_n is a product of 2-cycles of the form $(i,i+1)$ where $i<n$.
We will argue by induction on $b-a$ that (a,b) is a product of 2-cycles $(i,i+1)$.
Without loss of generality we can say $a>b$ since if $b>a$ we can simply interchange a,b in the following argument.
Basic Step: This is obvious when $b-a=1$, since $(a,b)=(a,a+1)$ is one of 2-cycles we want in the desired generating set.
Inductive Step: Now we suppose any 2-cycle (a,b) with $b-a=k,\ k>1$, can be written as a product of 2-cycles of the form $(i,i+1)$. Note that, under this choice, $(a,b)=(a,a+k)$.
Induction Step: Consider a 2-cycle (a,b) with $b-a=k+1$, that is,
$(a,b)=(a,a+k+1)$. We need to show (a,b) is the product of 2-cycles of the form $(i,i+1)$. Now (the multiplication is left to the reader),

$$(a,b)=(a+1,b)(a,a+1)(a+1,b)$$

The middle 2-cycle lies in our desired generating set. The first and third 2-cycles satisfy $b-(a+1)=b-a-1=k+1-1=k$ and therefore by supposition they can be written as a product of 2-cycles of the form $(i,i+1)$ and therefore so can (a,b). □

Theorem 14. *****
Every permutation in S_n can be written as a product of powers of $(1,2,\ldots,n)$ and (1,2).

Proof. Let $\sigma=(1,2)$ and $\rho=(1,2,\ldots,n)$.
Then,

$$\begin{aligned}\rho^2&=(3,4,,\ldots,n-1,n,1,2);\\ \rho^3&=(4,\ldots,n-1,n,1,2,3);\\ \rho^4&=(5,\ldots,n-1,n,1,2,3,4)\end{aligned}$$

This works like a clock. For ρ^k each element "steps forward" by k steps from its position in ρ. Clearly, $\rho^n=\rho_0$, the identity, but more importantly, for our purposes,

$$\rho^{n-1}=(1,n,n-1,\ldots,2)$$

Then we can compute to show,

$$\rho\sigma\rho^{n-1}=(1,2,\ldots,n)(1,2)((1,n,n-1,\ldots,2)=(2,3)$$

and in general,

$$\rho(i,i+1)\rho^{n-1}=(i+1,i+2)$$

So we have $(1,2)$ and $(2,3)$ and by $\rho(i,i+1)\rho^{n-1} = (i+1,i+2)$ we can produce,

$$\rho(2,3)\rho^{n-1} = (3,4)$$
$$\rho(3,4)\rho^{n-1} = (4,5), etc.$$

Therefore the product of powers of ρ, σ generate all 2-cycles of the form $(i,i+1)$. By Theorem 13 on page 49 they generate all permutations in S_n. □

Chapter 4

Group Theory Part III

Homomorphisms, Isomorphisms

In this chapter we begin our investigation of functions that operate on groups, we call them homomorphisms and isomorphisms.

4.1 Homomorphisms

Definition 25. *group homomorphism*
A group homomorphism ϕ maps elements in the group G_1 onto another group G_2. We write,

$$\phi : G_1 \to G_2,$$

where ":" is read as "maps" and "$\to$" as "onto". A group homomorphism obeys the rule,

$$\phi(a * b) = \phi(a) \otimes \phi(b)$$

for all $a, b \in G_1$, where the respective group operations on G_1 and G_2 are $*$ and $\otimes$.

Note that the operation $*$ is being taken in G_1 while the operation $\otimes$ is being taken in G_2. For simplicity we simply say ϕ is a homomorphism of groups if,

$$\phi(ab) = \phi(a)\phi(b) \ for \ all \ a, b \in G_1.$$

Example 31. *The map $\phi : \mathbb{Z} \to \mathbb{Z}$ with $\phi(n) = 5n$ is a homomorphism since,*

$$\phi(m+n) = 5(m+n) = 5m + 5n = \phi(m) + \phi(n) \qquad \diamond$$

Example 32. *The map $\phi : \mathbb{Z} \to < a >$ given by $\phi(n) = a^n$ is a homomorphism since*

$$\phi(m+n) = a^{m+n} = a^m a^n = \phi(m)\phi(n)$$

Note the operation in $\mathbb{Z}$ is addition but in $< a >$ the operation is multiplication. $\diamond$

For composite maps we have Theorem 15 that for any groups G_1, G_2, G_3 and homomorphisms $\phi : G_1 \to G_2, \psi : G_2, \to G_3$, the composite map $\phi \circ \psi$, or simply $\phi\psi$, is a homomorphism from G_1 to G_3.

Theorem 15. ****
For any groups G_1, G_2, G_3 and homomorphisms $\phi : G_1 \to G_2, \psi : G_2, \to G_3$, the composite map $\phi \circ \psi$ is a homomorphism from G_1 to G_3.

Proof. We need to show,

$$\phi \circ \psi(xy) = \phi \circ \psi(x)\phi \circ \psi(y).$$

We use the Definition 19 on page 37 of composition of functions and Definition 25 on page 52 of homomorphisms, namely,

$$f \circ g(x) = f(g(x)) \text{ and } \phi(ab) = \phi(a)\phi(b) \text{ and } \psi(cd) = \psi(c)\psi(d)$$

Accordingly,

$$\phi \circ \psi(xy) = \phi(\psi(xy)) = \phi(\psi(x)\psi(y))) = \phi(\psi(x))\phi(\psi(y)) = \phi \circ \psi(x)\phi \circ \psi(y))$$

□

Theorem 16 gives us various properties of homomorphisms.

Theorem 16. **** (Properties of homomorphisms)*
Let $\phi : G_1 \to G_2$ be a homomorphism. Then,

1. *$\phi(e_1) = e_2$ where e_1, e_2 are the respective identity elements.*
2. *$\phi(a^{-1}) = \phi(a)^{-1}$*
3. *$\phi(a^n) = \phi(a)^n$ for all $n \in \mathbb{Z}$.*
4. *If $a \in G$ and the order $|a|$ is finite, then $|\phi(a)| = |a|$.*
5. *If H is a subgroup of G_1 then $\phi(H) = \{\phi(h) | h \in H\}$ is a subgroup of G_2.*

Proof. We use $xe = x, ee = e$ and $\phi(x)\phi(y) = \phi(xy)$.

1. We want to show $\phi(e_1) = e_2$
   Note $\phi(e_1) \in G_2$ which has identity e_2 and hence $\phi(e_1)e_2 = \phi(e_1)$. But also,

   $$\phi(e_1)\phi(e_1) = \phi(e_1e_1) = \phi(e_1)$$

   hence,

   $$\begin{aligned} \phi(e_1)\phi(e_1) &= \phi(e_1)e_2 \\ \Rightarrow \phi(e_1) &= e_2 \end{aligned}$$

   by cancellation.

2. We want to show $\phi(a^{-1}) = \phi(a)^{-1}$
   We have,

   $\phi(a)\phi(a^{-1}) = \phi(aa^{-1}) = \phi(e_1) = e_2$ by (1), but also,
   $\phi(a)\phi(a)^{-1} = e_2$. Thus,
   $\phi(a)\phi(a)^{-1} = \phi(a)\phi(a^{-1})$
   so $\phi(a)^{-1} = \phi(a^{-1})$ by cancellation.

3. We want to show $\phi(a^n) = (\phi(a))^n$ for all $n \in \mathbb{Z}$. We have,

$$\begin{aligned}\phi(a^n) &= \phi(\overline{a.a.a.a.\ldots.a.a} \times a)\\ &= \phi(\overline{a.a.a.a.\ldots.a.a})\phi(a)\\ &= \phi(\overline{a.a.a.a.\ldots.a} \times a)\phi(a)\\ &= \phi(\overline{a.a.a.a.\ldots.a})\phi(a)^2\\ &\vdots\\ &= \phi(a)^n\end{aligned}$$

4. We want to show if $a \in G$ and the order[1] of $|a|$ is finite, then $|\phi(a)| = |a|$.
   We first claim that if G is a group and $a \in G$ is an element of finite order, say $|a| = n$, (see Definition 13 on page 33) then for any $k \in \mathbb{Z}$, we have $a^k = e$ if and only if $n|k \Leftrightarrow k = nm$ for some integer m. That is, n is the smallest integer for which $a^n = e$.
   Proof of the claim
   Suppose $n|k \Leftrightarrow k = nm$. We want to prove $a^k = e$. Then,

$$a^k = a^{nm} = (a^n)^m = e^m = e.$$

$$*****$$

   Conversely, suppose for any $k \in \mathbb{Z}$, that $a^k = e$. We want to prove $n|k$.
   Dividing k by n we can write[2] for some $b \in \mathbb{Z}$,

$$k = nb + c, 0 \leq c < n.$$

   Then,

$$e = a^k = a^{nb+c} = (a^n)^b a^c = a^c,\ 0 \leq c < n$$

   But $a^c = e$ with $c < n$ contradicts Definition 13 on page 33 that $|a| = n$ where n is the smallest integer such that $a^n = e$.
   Therefore $c = 0$ and $k = nb \Rightarrow n|k$. Thus n is the smallest integer for which $a^n = e$ and our claim has been proved.

[1] When reading $|a|$ or $|\phi(a)|$ remember this is the order of a or $\phi(a)$, that is the smallest integer n such that $a^n = e_1$ or $\phi(a)^n = e_2$.

[2] By the Division Algorithm Theorem 57A on page 105

*****

To prove $|\phi(a)| = |a|$, let $|a| = n \Leftrightarrow a^n = e$. Then by (3) we have,

$$\phi(a)^n = \phi(a^n) = \phi(e_1) = e_2.$$

By the claim we just proved above, n must be the smallest integer for which,

$$\phi(a)^n = e_2 \Rightarrow |\phi(a)| = n,$$

which is also $|a|$.

5. We want to show if H is a subgroup of G_1 then $\phi(H) = \{\phi(h)|h \in H\}$ is a subgroup of G_2.
To apply the subgroup test, Corollary 3 on page 31, we need to show that if,

$$\phi(a), \phi(b) \in \phi(H) \text{ then } \phi(a)\phi(b)^{-1} \in \phi(H).$$

Let $a, b \in H$. Then $\phi(a), \phi(b) \in \phi(H)$.
Since H is a subgroup, $ab^{-1} \in H$ so that $\phi(ab^{-1}) \in \phi(H)$.
But $\phi(ab^{-1}) = \phi(a)\phi(b)^{-1}$ so $\phi(a)\phi(b)^{-1} \in \phi(H)$ which is the subgroup test.

□

4.2 Kernel

The elements of the first group that are mapped onto the identity element of the second group by a homomorphism are important. We define,

Definition 26. *kernel of a group function*
Let $\phi : G_1 \to G_2$ be a group function and e_2 be the identity in G_2. Then the kernel of ϕ is the set,

$$ker(\phi) = \{x \in G_1 \mid \phi(x) = e_2\},$$

in other words the elements of G_1 that are mapped onto the identity of G_2.

Example 33. *The identity in $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ is 0 and any integer divisible by 5 becomes 0 under the modulo 5 operation. Hence, the kernel of $\phi : \mathbb{Z} \to \mathbb{Z}_5$ is,*

$$\{n \in \mathbb{Z} \mid n(\text{mod}5) \equiv 0, \text{ or } 5|n\} = \{0, \pm 5, \pm 10, \ldots\} = 5\mathbb{Z} \quad \diamond$$

We prove two theorems relating to the kernel, namely,

Theorem 17. *****
Let $\phi : G_1 \to G_2$ be a homomorphism. Then $ker(\phi)$ is a subgroup of G_1.

Proof. To prove $ker(\phi) = \{x \in G \mid \phi(x) = e_2\}$ is a subgroup of G_1, we need, according to Corollary 3 on page 31, to show if $a, b \in ker(\phi)$ then so does ab^{-1}, that is $\phi(ab^{-1}) = e_2$. Now if,

$$a, b \in ker(\phi) = \{x \in G_1 \mid \phi(x) = e_2\}$$

then by definition of the kernel, $\phi(a) = \phi(b) = e_2$.
But, since ϕ is a homomorphism,

$$\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(a)\phi(b)^{-1} = e_2 e_2^{-1} = e_2 \Rightarrow ab^{-1} \in ker(\phi).$$

Note the inverse of the identity is the identity. □

Theorem 18. *****
Let $\phi : G_1 \to G_2$ be a homomorphism. Then ϕ is one-to-one if and only if the kernel is trivial, that is, $ker(\phi) = \{e_1\}$ or the kernel contains only the identity element of G_1.

Proof. Suppose ϕ is one-to-one. We want to show $ker(\phi) = \{e_1\}$.
Let $x \in ker(\phi) = \{x \in G_1 \mid \phi(x) = e_2\}$. Suppose $\phi(x) = e_2$. But $\phi(e_1) = e_2$ by Theorem 16, page 53, so since ϕ is one to one and $\phi(x) = \phi(e_1)$, by Definition 16 on page 36 of a one-to-one function, we must have $x = e_1$.
So only e_1 is mapped onto e_2 and therefore,

$$ker(\phi) = \{x \in G_1 \mid \phi(x) = e_2\} = \{e_1\}.$$

*****

Conversely, suppose $ker(\phi) = \{e_1\}$ and suppose for some $x, y \in G_1$ that $\phi(x) = \phi(y)$. To prove ϕ is one-to-one we need to prove $x = y$. But,

$$\begin{aligned}
\phi(xy^{-1}) &= \phi(x)\phi(y^{-1}) \\
&= \phi(y)\phi(y^{-1}) \quad \text{using} \quad \phi(x) = \phi(y) \\
&= \phi(yy^{-1}) \\
&= \phi(e_1) \\
&= e_2 \\
&\Rightarrow xy^{-1} \in ker(\phi) = \{e_1\} \\
&\Rightarrow xy^{-1} = e_1 \\
&\Rightarrow xy^{-1}y = e_1 y \\
&\Rightarrow x = y.
\end{aligned}$$

So ϕ is one-to-one. □

4.3 Isomorphisms

We are particularly interested in group homomorphisms that cause two groups G_1 and G_2 to have the same "shape", specifically,

- the same number of elements,
- the same order for corresponding elements (that is, if $a^n = e_1$, the identity of G_1, then $|\phi(a)|^n = e_2$, the identity element of G_2.)
- preserve properties such as both groups are abelian or both are cyclic
- preserve products, identity elements and inverses like this,
  - Products: $\phi(a_1 a_2 \dots a_n) = \phi(a_1)\phi(a_2)\dots\phi(a_n)$
  - Identity: $\phi(e_1) = e_2$
  - Inverses: If $aa^{-1} = e_1$, then $\phi(a)\phi(a^{-1}) = e_2$.

Briefly expressed, we define such homomorphisms as isomorphisms and we prove there will be the same "shape" between two groups where the isomorphism $\phi : G_1 \Rightarrow G_2$ is a homomorphism satisfying,

$$\phi(ab) = \phi(a)\phi(b) \text{ for all } a, b \in G_1,$$

and is a one-to-one correspondence which we defined earlier. Put simply, a one-to-one correspondence means the mapping makes every element of G_1 correspond to exactly one element of G_2 and every element of G_2 correspond to exactly one element of G_1. The technical expression is that for an isomorphism we require ϕ to be one-to-one and onto or a one-to-one correspondence as well as being a homomorphism.

Definition 27. *group isomorphism*
We say $\phi : G_1 \to G_2$ is an isomorphism mapping group $(G_1, \otimes)$ onto the group $(G_2, \odot)$ if the following three conditions are satisfied,

- *$\phi(a \otimes b) = \phi(a) \odot \phi(b)$ for all $a, b \in G_1$, (that is, ϕ is a group homomorphism)*
- *ϕ is one-to-one, that is, if $\phi(a) = \phi(b)$ then $a = b$.*
- *ϕ is onto, that is, for every element $b \in G_2$ there is a corresponding element $a \in G_1$ such that $\phi(a) = b$.*

Note that since an isomorphism is a homomorphism, all the theorems for the properties of homomorphisms (specifically, Theorems 15, 16, 17 and 18) also apply to isomorphisms.

Definition 28. *isomorphic groups*
If an isomorphism $\phi : G_1 \to G_2$ exists then we say G_1, G_2 are isomorphic groups and we use the symbol,

$$G_1 \cong G_2.$$

Note 7. *Note that if we want to prove two groups are isomorphic (which we will do multiple times in this book), we need to conjecture or guess what the function could be and then prove the function is a homomorphism and is one-to-one and onto. Theorem 27 will be our first example of this set of steps. First, in Theorems 19 and 20 we prove the further properties we wished isomorphisms to have.*

Theorem 19. *****
Any group isomorphism preserves products, the identity element and inverses. Specifically,

1. $\phi(a_1a_2\dots a_n) = \phi(a_1)\phi(a_2)\dots\phi(a_n)$
2. $\phi(e_1) = e_2$ *where* e_1, e_2 *are the respective identity elements.*
3. $\phi(a)^{-1} = \phi(a^{-1})$ *for all* $a \in G_1$.

Proof. 1. We use induction to prove $\phi(a_1a_2\dots a_n) = \phi(a_1)\phi(a_2)\dots\phi(a_n)$
Basis Step: Let S_n be the statement $\phi(a_1a_2\dots a_n) = \phi(a_1)\phi(a_2)\dots\phi(a_n)$
Now $S_1 : \phi(a_1) = \phi(a_1)$ is trivially true but also $S_2 : \phi(a_1a_2) = \phi(a_1)\phi(a_2)$ is true by definition.
Induction Step: We assume $S_n : \phi(a_1a_2\dots a_n) = \phi(a_1)\phi(a_2)\dots\phi(a_n)$ is true.
We need to show $S_{n+1} : \phi(a_1a_2\dots a_na_{n+1}) = \phi(a_1)\phi(a_2)\dots\phi(a_n)\phi(a_{n+1})$ is true.

$$\begin{aligned}
\text{Left side} &= \phi(a_1a_2\dots a_na_{n+1}) \\
&= \phi(\overbrace{a_1a_2\dots\ a_n}a_{n+1}) \\
&= \phi(\overbrace{a_1a_2\dots\ a_n})\phi(a_{n+1}) \text{ by definition} \\
&= \phi(a_1)\phi(a_2)\dots\phi(a_n)\phi(a_{n+1}) \text{ by the assumption} \\
&= \text{Right side}
\end{aligned}$$

2. See Theorem 16 on page 53.
3. See Theorem 16.

□

Theorem 20. **** (Properties of Isomorphic Groups)*
Let $G_1 \cong G_2$. *Then,*

1. $|G_1| = |G_2|$, *that is they have the same number of elements.*
2. $|a| = |\phi(a)|$ *for all* $a \in G_1$, *that is their respective elements have the same order.*
3. G_1 *is abelian if and only if* G_2 *is abelian.*
4. G_1 *is cyclic if and only if* G_2 *is cyclic.*

Proof. Let $\phi : G_1 \to G_2$ be the isomorphism making $G_1 \cong G_2$.

1. We want to prove $|G_1| = |G_2|$, that is the two groups have the same number of elements.
   Now ϕ is a one-to-one and onto map between G_1 and G_2 (Refer Definitions 16 on page 36 and 17 on page 36). First suppose G_2 has more elements than G_1. Since ϕ is onto, all the elements in G_2 must be the mapping of an element in G_1. This must mean that there is an element (or several elements), say $a \in G_1$, that maps onto two different elements, say $g_1, g_2 \in G_2$ with $\phi(a) = g_1, \phi(a) = g_2$. But this contradicts Definition 15 on page 35 of a function, namely every element of the first set must map into exactly one element of the second set.
   On the other hand, suppose G_1 has more elements than G_2. Since ϕ is onto, every element of G_2 is a mapping of an element of G_1, but this must mean at least one element of G_2, say g_2, has been mapped onto by two different elements of G_1, say,

   $$a, b \in G_1, a \neq b \text{ and } \phi(a) = \phi(b) = g_2 \in G_2$$

   But in turn, this contradicts the fact that ϕ is one-to-one, whose Definition 16 on page 36, is that if $\phi(a) = \phi(b)$ then $a = b$.[3]

2. We want to prove $|a| = |\phi(a)|$ for all $a \in G_1$, that is their respective elements have the same order.
   This is proved in Theorem 16 (Properties of Homomorphisms), part (4) on page 53, since an isomorphism is also a homomorphism.

3. We want to prove G_1 is abelian if and only if G_2 is abelian.
   Suppose G_1 is abelian. Let $x, y \in G_2$. We need, according to Definition 6 on page 26, to show $xy = yx$.
   Since ϕ is onto, there are elements $a, b \in G_1$ such that $\phi(a) = x, \phi(b) = y$.
   Then since G_1 is abelian making $ab = ba$,

   $$xy = \phi(a)\phi(b) = \phi(ab) = \phi(ba) = \phi(b)\phi(a) = yx,$$

   so that G_2 is also abelian.

   *****

   Conversely suppose G_2 is abelian. Let $x, y \in G_2$, say $x = \phi(a), y = \phi(b)$ for some $a, b \in G_1$. Then,

   $$xy = yx \Rightarrow \phi(a)\phi(b) = \phi(b)\phi(a) \Rightarrow \phi(ab) = \phi(ba) \Rightarrow ab = ba$$

   so G_1 is also abelian.

[3] We have now formally proved the earlier statement following Definition 18 on page 36 that the simple way to remember the definition of a one-to-one correspondence between the elements of two finite sets is that it is a function where every element of the first set is paired with exactly one element of the second set and every element of the second set is paired with exactly one element of the first set.

4. We want to prove G_1 is cyclic if and only if G_2 is cyclic.
   We use Theorem 4 (3) on page 33 which states "a finite group G is cyclic if and only if there is an element $a \in G$ such that $|a| = |G|$."
   Suppose $G_1 =< a >$ is cyclic. Then $|a| = |G_1|$ by Theorem 10 (3).
   By (1) and (2) above,

$$|G_2| = |G_1| = |a| = |\phi(a)|$$

   so $|G_2| = |\phi(a)|$ and therefore $G_2 =< \phi(a) >$ is cyclic by Theorem 4 (3).

*****

   Conversely, suppose $G_2 =< b >$ is cyclic so that $|b| = |G_2|$. Then since ϕ is onto there is an $a \in G_1$ with $\phi(a) = b$ giving $|\phi(a)| = |b|$.
   But then,

$$|a| = |\phi(a)| = |b| = |G_2| = |G_1| \text{ by (1) and (2) above,}$$

   making $|G_1| = |a|$ and therefore G_1 is cyclic, again by Theorem 4 (3).

□

Note 8. *Let's return to how we prove two groups are isomorphic. To prove, for example, that all cyclic groups of the same number of elements n are isomorphic to each other and also to $\mathbb{Z}_n$, we need to conjecture (an educated guess!) a function ϕ between the two respective groups G_1, G_2 and then prove it is an isomorphism by proving it is one-to-one and onto and that $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G_1$. A simple example is to prove Theorem 21 that,*

$$\phi : \{e_1, a, a^2, \ldots, a^n\} \to \{e_2, b, b^2, \ldots, b^n\},$$

is an isomorphism between the cyclic groups $< a >, < b >$ of order n, where we conjecture $\phi(a^i) = b^i$ for $1 \leq n \leq n$.

Theorem 21. *****
Let $G_1 =< a >, G_2 =< b >$ be cyclic groups of the same finite order n. Then there is an isomorphism $\phi : G_1 \to G_2$ so that $G_1 \cong G_2$.

Proof. Let $G_1 =< a >= \{e, a, a^2, \ldots, a^{n-1}\}$, $G_2 =< b >= \{e, b, b^2, \ldots, b^{n-1}\}$ where the elements are all distinct.
Define (here is the educated guess) $\phi : G_1 \to G_2$ by $\phi(a^i) = b^i$ for $1 \leq i \leq n$.
We need to prove ϕ is one-to-one, onto and a homomorphism.

1. ϕ is clearly onto[4], since for each $b^i \in G_2$ there is an $a^i \in G_1$ such that $\phi(a^i) = b^i$.

[4]Definition 17, page 36

2. ϕ is one-to-one[5] since if $\phi(a^i) = \phi(a^j)$ then $b^i = b^j$, but since the elements are all distinct we must have $i = j$, so that $a^i = a^j$.

3. ϕ is a homomorphism[6] since,

$$\phi(a^i a^j) = \phi(a^{i+j}) = b^{i+j} = b^i b^j = \phi(a^i)\phi(a^j).$$

We conclude ϕ is an isomomorphism and $G_1 \cong G_2$. □

Of course we could have simply claimed the one-to-one correspondence (one-to-one and onto) due to the obvious fact that both groups have the same number n of elements.
Finally, we prove in Corollary 22 that if $G =< a >$ is a cyclic group with $|G| = n$ then we have the isomorphism given by,

$$G \cong \mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}.$$

Corollary 22. ***
Let $G =< a >$ be a cyclic group. If $|G| = n$ then $G \cong \mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$.

Proof. This is true by Theorem 21 since we have two cyclic groups of the same order. □

Of course we are saying $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ is cyclic but this is just the definition of a cyclic group since $\mathbb{Z}_n =< 1 >$ under the operation addition modulo n.

[5]Definition 16, page 36
[6]Definition 27, page 57

Chapter 5

Group Theory Part IV

Cosets, Normal Groups, Factor Groups

5.1 Cosets

Definition 29. *cosets*
The set of (left) cosets $a * H$ of a subgroup H of a group $(G, *)$ determined by an element $a \in G$ is,

$$a * H = \{x \in G \mid x = a * h \text{ for some } h \in H\}$$

If the operation $*$ is addition, $a * H$ means we are adding a to every element of H. If the operation is multiplication, $a * H$ means we are multiplying every element of H by a.
The set of right cosets is $H * a$.

Definition 30. *index*
The number of left cosets of H in G is called the index of H in G and is denoted by $[G : H]$.

Example 34. *Let us consider $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ and $H = \{0, 3\}$ under addition modulo 6.*
We first prove closure, associativity and the existence of an identity and inverses and that $H = \{0, 3\}$ is a subgroup of $\mathbb{Z}_6$.

- *Closure:* $0 + 0 \in H; 0 + 3 = 3 \in H : 3 + 3 = 0 \in H$
- *Identity: 0*
- *Inverses: The pairs are* $0 + 0 = 0,\ 3 + 3 = 0$
- *Associativity: 0,3 are integers and integers have associativity*

Since there are 6 possible values for $x \in \mathbb{Z}_6$*, there are therefore 6 possible cosets of* $H = \{0, 3\}$ *in* $\mathbb{Z}_6$ *under addition modulo 6, namely,*

$$\begin{aligned}
0 + H &= \{0, 3\} = H \\
1 + H &= \{1, 4\} \\
2 + H &= \{2, 5\} \\
3 + H &= \{3 (\text{mod } 6), 6 (\text{mod } 6)\} = \{3, 0\} = H \\
4 + H &= \{4, 1\} = 1 + H \\
5 + H &= \{5, 2\} = 2 + H
\end{aligned}$$

So there are just three cosets: $H, 1 + H$ *and* $2 + H$ *and we write* $[\mathbb{Z}_6 : H] = 3$. ◇

Note 9. *We note that the three cosets* $0 + H = \{0, 3\},\ 1 + H = \{1, 4\},\ 2 + H = \{2, 5\}$ *partition the group into three disjoint subsets, no elements in common. No two cosets have the same elements and each contains exactly the same number of elements as* H*.*

Let's consider another example, this time with multiplication modulo 11.

Example 35. *Let* $G = \mathbb{Z}_{11}^{\times}$ *under multiplication modulo 11.*
Let $H = \{1, 10\}$*. Then* H *is a subgroup since the axioms of Definition 5 on page 25 are satisfied. We have,*

(a) Closure: $1 \times 1 = 1 \in H, 1 \times 10 = 10 \in H, 10 \times 10 = 1 \in H$.

(b) Identity element is 1

(c) Associativity is true since the elements are integers.

(d) Inverses: The two elements 1,10 are their own inverses, since $1 \times 1 = 1, 10 \times 10 = 1$.

Using multiplication modulo 11, $[\mathbb{Z}_{11}^{\times} : H] = 5$ *since the cosets are:*

$$\begin{aligned}
1H &= \{1, 10\} = H \\
2H &= \{2, 20\} = \{2, 9\} \\
3H &= \{3, 30\} = \{3, 8\} \\
4H &= \{4, 40\} = \{4, 7\} \\
5H &= \{5, 50\} = \{5, 6\} \\
6H &= \{6, 60\} = \{6, 5\} = 5H \\
7H &= \{7, 70\} = \{7, 4\} = 4H \\
8H &= \{8, 80\} = \{8, 3\} = 3H \\
9H &= \{9, 90\} = \{9, 2\} = 2H \\
10H &= \{10, 100\} = \{10, 1\} = 1H = H
\end{aligned}$$ ◇

Note 10. *Again note that in both of these examples the cosets partition the set G into disjoint subsets. All the elements of G may be found in the cosets and none are repeated.*
Note also that since every coset aH contains exactly the elements of H operated on by a that each coset has exactly the same number of elements as H.
To be rigorous, we can define the map $\mu : H \to aH$ by $\mu(h) = ah$ which is,

- *onto ($ah \in aH$ corresponds to $h \in H$)*
- *one-to-one ($ah_1 = ah_2 \Rightarrow h_1 = h_2$ by cancellation),*

so μ is a one-to-one correspondence and H and aH must have the same number of elements.

*****

To show no element can be in more than one coset, let H be a subgroup of G and suppose a, b, c are elements of G such that $b \notin aH$ and c is in both aH and bH. Then there are elements such that $c = ah_1$ and $c = bh_2 \Rightarrow ah_1 = bh_2 \Rightarrow b = ah_1h_2^{-1}$. But $h_1h_2^{-1} \in H \Rightarrow b \in aH$ which is a contradiction. Thus, no element can be in more than one coset.

Using the symbol $[G : H]$ for the number of left cosets of H in G we prove Lagrange's Theorem.

Theorem 23. ** (Lagrange)*
Let G be a group of finite order (finite number of elements) and H a subgroup of G. Then the order of H divides the order of G. Indeed $\frac{|G|}{|H|} = [G : H]$. In addition, if $a \in G$ then the order $|a|$ of a divides the order $|G|$ of G.

Proof. Let H be a subgroup of the finite group G.
By Definition 29 on page 62, the number of cosets of H is $[G : H]$ and by Note 10 above, each coset has $|H|$ elements.
The cosets are all disjoint and no element of G is omitted, hence altogether the cosets contain $[G : H] \times |H|$ elements and this is $|G|$. Hence $\frac{|G|}{|H|} = [G : H]$ so the order of H divides the order of G.

*****

By Theorem 4 (1) on page 33 $< a >$ is a subgroup of G, so by what we have just proved, $| < a > |$ divides $|G|$.
But, by Theorem 4 (2), $|a| = | < a > |$, so $|a|$ divides $|G|$. □

5.2 Normal Subgroups

Definition 31. *normal subgroup*
We define a subgroup H of a group G to be a normal subgroup if,

$$ghg^{-1} \in H \text{ for all } h \in H \text{ and } g \in G.$$

that is if there is an element $h_1 \in H$ such that $ghg^{-1} = h_1$.

Notation 3. *If H is a normal subgroup of G we write $H \lhd G$ if H is a proper subgroup of G and $H \trianglelefteq G$ if it may be either a proper subgroup or the whole of G.*

Note 11. *Since $ghg^{-1} \in H \Rightarrow ghg^{-1} = h_1$ for some $h_1 \in H$, we have $g^{-1}ghg^{-1}g = g^{-1}h_1g$ so that $g^{-1}h_1g = h$. Accordingly some writers define H to be normal if $g^{-1}hg \in H$ for all $h \in H$ and $g \in G$. Their subsequent results are the same as those deriving from our definition.*

Easy examples of normal groups are provided by Theorem 24.

Theorem 24. ****
Let G be a group with identity element e and let H be a subgroup of G.

1. *If $H = G$ then H is normal (a normal subgroup of G).*
2. *If $H = \{e\}$ then H is normal.*
3. *If G is abelian then H is normal.*

Proof. In each case we need to prove Definition 31 on page 65 holds, that $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$.

1. Let $H = G$. Now $ghg^{-1} \in G$ but $G = H$ so $ghg^{-1} \in H$ making $H \lhd G$.
2. Let $H = \{e\}$ and $g = e, h = e$ in ghg^{-1}.
   Then $eee^{-1} = e \in H$ so $H \lhd G$.
3. Suppose G is abelian.[1] If $h \in H$ and $g \in G$ then,

$$\begin{aligned} ghg^{-1} &= g(hg^{-1}) = g(g^{-1}h) \text{ since } G \text{ is abelian} \\ &= (gg^{-1})h = eh = h \\ &\Rightarrow ghg^{-1} \in H \text{ since we assumed } h \in H \\ &\Rightarrow H \lhd G. \end{aligned}$$

□

[1] Definition 6, page 26

Theorem 25 proves the left and right cosets are the same or $aH = Ha$ if and only if and only if $aha^{-1} \in H$ for all $h \in H$ and $a \in G$, that is, if and only if $H \triangleleft G$.

Theorem 25. *
Consider a subgroup H of a group G and let $a \in G$. Then $aH = Ha$ if and only if $aha^{-1} \in H$ for all $h \in H$ and $a \in G$. That is, H is a normal subgroup of G or $H \triangleleft G$ if and only if $aH = Ha$ for all $a \in G$.

Proof. Suppose $aH = Ha$ for all $a \in G$. We need to prove that for any $h \in H$ that $aha^{-1} \in H$ so that $H \triangleleft G$.
Let $h \in H$. Now by the supposition, $aH = Ha$ for any $h \in H$, or $ah = h_1a$ for some $h_1 \in H$.
Hence, multiplying on the right by a^{-1}, $aha^{-1} = h_1aa^{-1}$ for some $h_1 \in H$.
But $aha^{-1} = h_1aa^{-1} \Rightarrow aha^{-1} = h_1e = h_1$, and since $h_1 \in H$ then so does aha^{-1}, making $H \triangleleft G$.

*****

Conversely, suppose $aha^{-1} \in H$ for all $h \in H$ and $a \in G$.
We will prove double containment, that is, $aH \subseteq Ha$ and $Ha \subseteq aH$ so that we must have $aH = Ha$.
First, we prove $aH \subseteq Ha$ by proving that any element $ah \in aH$ is also an element of Ha. We do this by proving $ah = h_2a$ for some $h_2 \in H$.
Now we have supposed $aha^{-1} \in H$. Then $aha^{-1} = h_2$ for some $h_2 \in H$.
Then multiplying by a,

$$aha^{-1}a = h_2a \Rightarrow ahe = h_2a \Rightarrow ah = h_2a \Rightarrow aH \subseteq Ha.$$

Second, we prove $Ha \subseteq aH$ by proving if $ha \in Ha$ then $ha = ah_3$ for some $h_3 \in Ha$.
Now by the assumption $xhx^{-1} \in H$ for all $h \in H$ and $x \in G$.
Let $x = a^{-1}$ and note $(a^{-1})^{-1} = a$. Then,

$$\begin{aligned} a^{-1}h(a^{-1})^{-1} \in H &\Rightarrow a^{-1}h(a^{-1})^{-1} = h_3 \text{ for some } h_3 \in H \\ &\Rightarrow aa^{-1}h(a^{-1})^{-1} = ah_3 \\ &\Rightarrow eha = ah_3 \\ &\Rightarrow ha = ah_3 \\ &\Rightarrow Ha \subseteq aH \end{aligned}$$

But $aH \subseteq Ha$ and $Ha \subseteq aH$ means we must have $aH = Ha$. □

$aH = Ha$ is certainly true when the group is abelian as we prove in Corollary 26.

Corollary 26. *
If a group G is abelian, the left and right cosets aH, Ha of the subgroup H of G are the same. Consequently any abelian subgroup is a normal subgroup.

Proof. If G is abelian and $h \in H$ and $a \in G$, then, using associativity and commutativity,

$$aha^{-1} = a(ha^{-1}) = a(a^{-1}h) = (aa^{-1})h = eh = h \in H$$

So by Theorem 25, $aH = Ha$ and H is a normal subgroup of G. □

Example 36. *$2\mathbb{Z} = \{0, \pm 2, \pm 4, \ldots\}$ is a subgroup of $\mathbb{Z}$.*
Then $2\mathbb{Z} \triangleleft \mathbb{Z}$ since, under addition, if $g \in \mathbb{Z}$ then $g^{-1} = -g$ and for any $h = 2k \in 2\mathbb{Z}$ we have,

$$ghg^{-1} = g + 2k - g = 2k \in 2\mathbb{Z}.$$

Or we could simply say $2\mathbb{Z}$ is abelian (since $\mathbb{Z}$ is) and use Theorem 24 (3), page 65.
◇

The fundamental theorem of Galois Theory, which is our penultimate goal, relies on normal subgroups. We have already proved in Theorem 12 on page 48 a relationship between the alternating subgroup A_n and the symmetric group S_n, namely $|A_n| = \dfrac{|S_n|}{2}$. We proceed to prove that in general via Theorems 27 and 28 that if H is a subgroup of a group G and the index $[G : H] = 2$ or $|H| = \dfrac{|G|}{2}$ then $H \triangleleft G$ or H is a normal subgroup of G. Accordingly, $A_n \triangleleft S_n$.

Theorem 27. ***
Let G be a group with subgroup H such that the index $[G : H] = 2$. Then H is a normal subgroup of G, or $H \triangleleft G$.

Proof. $[G : H] = 2$ means H has just two left cosets and two right cosets which, for any $g \in G$ can only be H, gH and H, Hg respectively.
But since the cosets partition G and the first partition in both cases is H then whether right or left, the other coset must be the remainder $G - H$ so we can only have $gH = Hg \Rightarrow H \triangleleft G$ by Theorem 25 on page 66. □

Theorem 28. ***
If G is a finite group and H is a subgroup of G where $|H| = \dfrac{|G|}{2}$ then H is a normal subgroup of G.

Proof. Suppose G is a finite group and H is a subgroup of G where $|H| = \dfrac{|G|}{2}$.
By Lagrange's Theorem 23 on page 64, $\dfrac{|G|}{|H|} = [G : H]$.
Then, given $|H| = \dfrac{|G|}{2}$ we have $[G : H] = 2$. So by Theorem 27, $H \triangleleft G$. □

To make use of these results we prove in Theorem 29 that the alternating group A_n of even permutations is a normal subgroup of S_n.

Theorem 29. *
The alternating group A_n of even permutations is a normal subgroup of S_n.

Proof. From Theorem 12 on page 48 we have $|A_n| = \frac{|S_n|}{2}$ so, by Theorem 28, A_n is a normal subgroup of S_n. □

That $A_n \triangleleft S_n$, or A_n is a normal subgroup of S_n, is once again a vital result for proving our ultimate goal, the insolvability by radicals of polynomials of degree ≥ 5.

5.3 Factor Groups.

In Example 34 on page 62 we found the cosets of $H = \{0, 3\}$ in $G = \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ to be $H, 1 + H, 2 + H$. We proceed to prove that in general the cosets of the subgroup H in the group G are themselves a group. We first define the operation we need to show the cosets form a group.

Definition 32. *coset multiplication*
For G a group, H a subgroup of G and $a, b \in G$, we define the operation of coset multiplication by,

$$(aH)(bH) = abH$$

To show this operation is well defined we need to show it does not depend upon the choice of a, b. We prove this in Theorem 31, that if we have a subset H of a set G, written $H < G$, and $a, b, c, d \in G$, then,

$$aH = cH \text{ and } bH = dH \Rightarrow abH = cdH \Rightarrow cHdH = abH.$$

The proof of Theorem 31 requires the result of Theorem 30.

Note 12. *Many mathematical theorems begin with TFAE, meaning,*

" **T***he* **F***ollowing (statements P, Q, R, etc.)* **A***re* **E***quivalent."*

The simplest case is $P \Leftrightarrow Q$ which means we must prove $P \Rightarrow Q$ and $Q \Rightarrow P$ or the two statements P, Q are equivalent.
To show P, Q, R are equivalent, we must prove $P \Leftrightarrow Q, Q \Leftrightarrow R, R \Leftrightarrow P$ but this will follow if we simply prove $P \Rightarrow Q, Q \Rightarrow R, R \Rightarrow P$.
And so on. In each case we begin with P and prove a cycle of implications that end up back with P.

Theorem 30. *****
Let H be a subgroup of G and let $a, b \in G$. Then, TFAE or the following conditions are equivalent (if any one is true, so are all the others)

1. $bH = aH$
2. $bH \subseteq aH$
3. $b \in aH$
4. $a^{-1}b \in H$

Proof. We have four implications to prove.
1. $\Rightarrow$ 2. We want to show $bH = aH \Rightarrow bH \subseteq aH$.
Proof: If a set equals another set then it is also true it is contained within that set.

*****

2. $\Rightarrow$ 3. We want to show $bH \subseteq aH \Rightarrow b \in aH$.
Proof: Now H is a subgroup of G, so by Theorem 2 on page 30 it has the same identity element e as G. Accordingly, given $bH \subseteq aH$ then $bh_1 = ah_2$ for some $h_1, h_2 \in H$ so that,

$$bh_1h_1^{-1} = ah_2h_1^{-1} \Rightarrow be = ah_3,\ h_3 = h_2h^{-1} \in H \Rightarrow b = ah_3 \Rightarrow b \in aH.$$

*****

3. $\Rightarrow$ 4. We want to show $b \in aH \Rightarrow a^{-1}b \in H$.
Proof: Now if $b \in aH$ then $b = ah$ for some $h \in H$ but then $a^{-1}b = a^{-1}ah = h \in H$.

*****

4. $\Rightarrow$ 1. We want to show $a^{-1}b \in H \Rightarrow bH = aH$.
Proof: If $a^{-1}b \in H \Rightarrow a^{-1}b = h$ for some $h \in H$, then by multiplying by inverses, we have the two equations,

$$a^{-1}b = h \Rightarrow aa^{-1}b = ah \Rightarrow eb = ah \Rightarrow b = ah \tag{5.3.1}$$
$$b = ah \Rightarrow bh^{-1} = ahh^{-1} \Rightarrow bh^{-1} = a \tag{5.3.2}$$

We will show $bH = aH$ by showing $bH \subseteq aH$ and $aH \subseteq bH$.
First let $x \in bH$.
We need to show $x \in aH$ or $x = ah,\ h \in H$, to conclude $bH \subseteq aH$.
Now $x \in bH \Rightarrow x = bh_1$ for some $h_1 \in H$.
Substituting (5.3.1) gives $x = ahh_1 \Rightarrow x \in aH$ since $hh_1 \in H$ so we have $bH \subseteq aH$.
Second let $x \in aH$.
We need to show $x \in bH$ or $x = bh,\ h \in H$, to conclude $aH \subseteq bH$.
Now $x \in aH \Rightarrow x = ah_2$ for some $h_2 \in H$.
Substituting (5.3.2) gives $x = bh^{-1}h_1 \Rightarrow x \in bH$ since $h^{-1}h_1 \in H$.
We conclude $bh \subseteq aH$ and together with $aH \subseteq bH$ this implies $bH = aH$. □

Theorem 31. **
Let $H \triangleleft G$ and $a, b, c, d \in G$. If $aH = cH$ and $bH = dH$ then $abH = cdH$.

Proof. Let $H \triangleleft G$ and $a, b, c, d \in G$.
If $aH = cH$ and $bH = dH$ then by Theorem 30 (1) $\Leftrightarrow$ (4) we have $a^{-1}c \in H$ and $b^{-1}d \in H$ for any $c, d \in H$.
Since H is a normal subgroup, by Definition 31 on page 65, $d^{-1}(a^{-1}c)d \in H$.
But we also have $bd^{-1} \in H$ so, since H is a group, by closure the product,

$$\begin{aligned}(b^{-1}d)d^{-1}(a^{-1}c)d \in H &\Rightarrow b^{-1}(dd^{-1})a^{-1}cd \in H \\ &\Rightarrow (b^{-1}a^{-1})cd \in H \\ &\Rightarrow (ab)^{-1}cd \in H \\ &\Rightarrow (ab)^{-1}cd = h \text{ for some } h \in H \\ &\Rightarrow cd = abh \\ &\Rightarrow cdH = abhH = abH \text{ since } hH = H.\end{aligned}$$

□

Note 13. *It is "obvious" that $hH = H$ but let's prove it anyway! Again we prove double containment, that is, $hH \subseteq H$ and $H \subseteq hH$.*
First, the multiple of every element of H by h is a set contained within H so $hH \subseteq H \Rightarrow hh^{-1} \subseteq hH$.
Second, if $h \in H$ then so does the inverse h^{-1} and again the multiple of every element of H by h^{-1} is a set contained within H so that $hh^{-1}H \subseteq hH$.
Then, $hh^{-1}H \subseteq hH \Rightarrow H \subseteq hH$ since $hh^{-1} = e$ and $eH = H$.
So, by double containment, $hH = H$.

Finally we can prove Theorem 32, that if H is a normal subgroup of G then the set of left cosets of H forms a group under coset multiplication $(aH)(bH) = abH$.

Theorem 32. *
If H is a normal subgroup of G then the set of left cosets of H forms a group under coset multiplication

$$(aH)(bH) = abH.$$

Proof. We need to prove the four group axioms (see Definition 5 on page 25) hold for $\{aH | a \in G\}$.

(i) Closure is shown by Theorem 31 above, that coset multiplication is well defined, that is, the product of two cosets gives another coset, irrespective of the choice of a, b.

(ii) The identity element[2] is the coset H since $eH = H$ so that, using Definition 39 on page 91 of coset multiplication, we have,

$$eHaH = eaH = aH \text{ and } aHeH = aeH = aH \text{ for all } a \in G.$$

[2]To show any e is the identity element of a group G we must show $ae = ea = a$ for all $a \in G$, which is Axiom 3 in Definition 5 of a group.

(iii) The inverse of aH is $a^{-1}H$ since,

$$aHa^{-1}H = aa^{-1}H = eH = H.$$

(iv) Associativity is true since if $a, b, c \in G$ then,

$$(aHbH)cH = abHcH = abcH = a(bc)H = aH(bcH) = aH(bHcH)$$

Hence $\{aH|a \in G\}$ is a group. □

Definition 33. *factor group*
If H is a normal subgroup of G, the group of left cosets of H is called the factor group of G on H. It is denoted by G/H and is the set $\{gH \mid g \in G\}$.

Some algebra books call G/H a quotient group. Employing modulo language, we also say the coset elements in G/H are the residue classes of G modulo H and we (loosely) refer to G/H as G *mod* H.

Example 37. *In Example 34 in Section 5.1, we had for $H = \{0, 3\}$ and $G = \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ that the set of cosets is,*

$$\begin{aligned}\mathbb{Z}_6/H &= \{a + \{0, 3\} \mid a \in \mathbb{Z}_6\} \\ &= \{\{0, 3\}, \{1, 4\}, \{2, 5\}\} \\ &= \{0 + H, 1 + H, 2 + H\}\end{aligned}$$

Again note,

$$\begin{aligned}3 + H &= 3 + (0, 3) = (3, 6) \equiv (0, 3) = H, \\ 4 + H &= 4 + (0, 3) = (4, 7) \equiv (1, 4) = 1 + (0, 3) = 1 + H, \\ 5 + H &= 5 + (0, 3) = (5, 8) \equiv (2, 5) = 2 + (0, 3) = 2 + H\end{aligned}$$

under addition modulo 6, so there are just 3 cosets.
Under the operation $(a + H)(b + H) = (a + b) + H$ we have the operations table,

	0+H	*1+H*	*2+H*
0+H	*0+H*	*1+H*	*2+H*
1+H	*1+H*	*2+H*	*0+H*
2+H	*2+H*	*0+H*	*1+H*

Clearly closure, associativity, the identity $(0 + H) = H$, and the three inverses $(1 + H + 2 + H = 0 + H$, etc.) are all demonstrated so $\mathbb{Z}_6/H$ is a group. ◇

5.4 Another notation for Cosets

5.4.1 Integers

Let us first consider an example.

Example 38. *As we found in Example 11 on page 31,* $3\mathbb{Z} = \{0, \pm 3, \pm 6, \pm 9, \ldots\}$ *is a subgroup of* $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$ *and, by Theorem 30 (3),* $3\mathbb{Z} \lhd \mathbb{Z}$ *since both are abelian.*
The left cosets of $3\mathbb{Z}$ *are* $0 + 3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}$ *since any other* $n + 3\mathbb{Z}$ *is simply a repetition of one of these, for example,* $31 + 3\mathbb{Z} = 1 + 3 \times 10 + 3\mathbb{Z} = 1 + 3\mathbb{Z}$.
Accordingly,

$$\mathbb{Z}/3\mathbb{Z} = \{0 + 3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}\}$$

The three cosets have separated the integers into three equal parts depending on whether the remainder when an integer is divided by 3 is $0, 1$ *or* 2.
We can use the following notation for the three cosets,

$$\begin{aligned}
[0]_3 &= 0 + 3\mathbb{Z} = \{0, \pm 3, \pm 6, \ldots\} \\
[1]_3 &= 1 + 3\mathbb{Z} = \{1, 4, 7, \ldots\} \cup \{-2, -5, -8, \ldots\} \\
[2]_3 &= 2 + 3\mathbb{Z} = \{2, 5, 8, \ldots\} \cup \{-1, -4, -7, \ldots\}
\end{aligned}$$

where we call $[0]_3, [1]_3, [2]_3$ *congruence classes and we then have,*

$$\mathbb{Z}/3\mathbb{Z} = \{[0]_3, [1]_3, [2]_3\}$$

Now, $\mathbb{Z}_3 = \{0, 1, 2\}$ *under addition modulo 3. We can then define an isomorphism,*

$$\phi : \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}_3 \text{ where } \phi(m + 3\mathbb{Z}) = m.$$

It is easy to see this function is one-to-one and onto. It is a homomorphism since,

$$\begin{aligned}
&\phi(m + 3\mathbb{Z} + n + 3\mathbb{Z}) \\
&= \phi(m + n + 3\mathbb{Z}) \\
&= m + n \\
&= \phi(m + 3\mathbb{Z}) + \phi(n + 3\mathbb{Z})
\end{aligned}$$

We conclude $\mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}_3$. ◇

Note 14. *In general,*

$$\begin{aligned}
\mathbb{Z}/n\mathbb{Z} &= \{a + n\mathbb{Z} \mid a \in \mathbb{Z}\} \\
&= \{[0]_n, [1]_n, \ldots, [n-1]_n\}
\end{aligned}$$

since when any integer is divided by n *the (least positive) remainders are* $0, 1, \ldots, n-1$.
We call $[0]_n, [1]_n, \ldots, [n-1]_n$ *the congruence classes of* 0 *to* $n-1$ *modulo* n. *We also note the relationship between* $\mathbb{Z}/n\mathbb{Z}$ *and* $\mathbb{Z}_n$, *since the above argument easily generalizes to* $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$. *Accordingly, some authors abuse the notation and use* $\mathbb{Z}_n$ *when they actually mean* $\mathbb{Z}/n\mathbb{Z}$.

5.4.2 Cosets for Groups in General

The set of (left) cosets $a * H$ of a subgroup H of a group $(G, *)$ determined by an element $a \in G$ is,

$$a * H = \{x \in G \mid x = a * h \text{ for some } h \in H\}$$

We can replace the symbol aH with simply $[a]$ which we call the congruence class of a. Accordingly we can write $G/H = \{aH \mid a \in G\} = \{[a_1], [a_2], \ldots [a_j]\}$ where any other $[a_k],\ k > j$ simply repeats one of the cosets $[a_1], [a_2], \ldots [a_j]$.
We then define the addition and multiplication of cosets by,

$$[a] + [b] = [a + b]$$
$$[a].[b] = [a.b]$$

Accordingly, by Theorem 32 on page 70, these operations are well defined.

5.5 Homomorphism Theorem for Groups

The factor groups we particularly need are related to the symmetric groups S_n and the subgroup, A_n, of even permutations. We need the definition of the kernel of an isomorphism, paralleling that for homomorphisms, and also the three isomorphism theorems.

Definition 34. *kernel of an isomorphism*
As for groups, the kernel of the isomorphism $\phi : G_1 \to G_2$, is the set of elements in the first group that are mapped onto the identity of the second group, thus,

$$ker(\phi) = \{x \in G_1 \mid \phi(x) = e_2 \in G_2\}$$

Theorem 33 is the Fundamental Homomorphism Theorem for Groups. It states that if G_1, G_2 are groups and $\phi : G_1 \to G_2$ is a group homomorphism with $K = ker(\phi)$ then we have the isomorphic groups,

$$G_1/K \cong \phi(G_1)$$

Theorem 33. **** (Fundamental Homomorphism Theorem or First Isomorphism Theorem for Groups)*
Let G_1, G_2 be groups. If $\phi : G_1 \to G_2$ is a group homomorphism with $K = ker(\phi)$ then

$$G_1/K \cong \phi(G_1)$$

Proof. Note the elements of G_1/K are $\{aK \mid a \in G_1\}$.
We need to find an isomorphism $\psi : G_1/K \to \phi(G_1)$

Let $a \in G_1$. For each coset $aK \in G_1/K$, define $\psi(aK) = \phi(a)$. To show ψ is well-defined[3] , we need to show its definition is independent of the choice of a. This means if $aK = bK$ then $\psi(aK) = \psi(bK) \Rightarrow \phi(a) = \phi(b)$.
Accordingly, ψ is well-defined since if $aK = bK$ for $a, b \in G_1$, then by Theorem 36 on page 78, $ab^{-1} \in K \Rightarrow ab^{-1} = k$ for some $k \in K$ or $a = bk$ and therefore,

$$\phi(a) = \phi(bk) = \phi(b)\phi(k) = \phi(b)e_2 = \phi(b) \text{ for all } a, b \in G_1.$$

***

Second, ψ is a homomorphism (see Definition 25, page 52) since, using coset multiplication, (Definition 33, page 71),

$$\psi(aKbK) = \psi(abK) = \phi(ab) = \phi(a)\phi(b) = \psi(aK)\psi(bK)$$

Third, to show ψ is one-to-one we need to show $\psi(aK) = \psi(bK) \Rightarrow aK = bK$. But,

$$\psi(aK) = \psi(bK) \Rightarrow \phi(a) = \phi(b),$$

and then, using the homomorphism and Theorem 16 (2), page 53 that
$\phi(a^{-1}) = \phi(a)^{-1}$,

$$\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(b)\phi(b)^{-1} = e_2.$$

Then, by Definition 34, page 73 of the kernel, $ab^{-1} \in K$, showing $aK = bK$ by Theorem 30, (4) $\Rightarrow$ (1) on page 69.
Thus ψ is one-to-one.
Fourth, ψ is clearly onto since each $\phi(a)$ has a corresponding $\psi(aK)$,
We conclude ψ is an isomorphism making $G_1/K \cong \phi(G_1)$. □

Note 15. *If $\phi : A \to B$ is a function then every element of A is mapped onto B. Thus we can write $\phi(A) \subset B$. But we cannot say $\phi(A) = B$ since there may be elements of B that are not mapped onto by ϕ.*
For example $\phi : \mathbb{N} \to \mathbb{Z}$, $\phi(n) = n^2$ is a function but $\phi(\mathbb{N}) \neq \mathbb{Z}$ since no negative integer is mapped onto by ϕ.
However, if $\phi : A \to B$ is an onto function then by definition of "onto", every element $b \in B$ is such that $\phi(a) = b$ for some element $a \in A$. In this case we do have $\phi(A) = B$. Specifically, while the Fundamental Homomorphism Theorem 33, page 73, states for $\phi : G_1 \to G_2$ that $G/K \cong \phi(G_1)$, we can have $G_1/K \cong G_2$, provided we first show ϕ is onto – and we will do that several times in what follows.

[3] A function is well-defined if it obeys Definition 15, page 35 of a function, namely $f : A \to B$ is a function if each element $a \in A$ maps onto only one $b \in B$, or equivalently, if $a, c \in A$ and $a = c$ then $f(a) = f(c)$, which is what we prove here by proving $aH = bH \Rightarrow \Omega(aH) = \Omega(bH)$.

5.6 Isomorphism Theorems for Groups

We now prove the remaining two of the three isomorphism theorems that we will need later.

Theorem 34. **** (Second Isomorphism Theorem)*
Let N be a normal subgroup of a group G, that is $N \triangleleft G$, and let H be a subgroup of G. Then,

a. $H \cap N \triangleleft H$.

b. HN *is a subgroup of* G.

c. $H/(H \cap N) \cong HN/N$.

Note $HN = \{hn \mid h \in H, n \in N\}$.

Proof. a. Show $H \cap N \triangleleft H$.
By Definition 31 on page 65 of a normal subgroup we need to show if $h \in H$ and $n \in H \cap N$ then $h^{-1}nh \in H \cap N$.
We are given $N \triangleleft G$ which means $gng^{-1} \in N$ for all $g \in G$ and $n \in N$.
Now if $n \in H \cap N$ then $n \in N$, and since $H \leq G$ if $h \in H$ then $h \in G$.
So $gng^{-1} \in N$ for all $g \in G$ means $hnh^{-1} \in N$ since $h \in G$.
Further $n \in H \cap N \Rightarrow n \in H$ as do h, h^{-1} and therefore, by the closure axiom of groups, the product $h^{-1}nh \in H$.
Therefore, $h^{-1}nh$ belongs to both H and N, so $h^{-1}nh \in H \cap N$ and we have proved $H \cap N \triangleleft H$.

b. Show HN is a subgroup of G.
By the subgroup test, Corollary 3 on page 31, to prove HN is a subgroup of G we need to show if $x_1, x_2 \in HN$ then $x_1x_2^{-1} \in HN$, that is $x_1x_2^{-1} = hn$ for some $h \in H$ and $n \in N$.
Let $x_1, x_2 \in HN \Rightarrow x_1 = h_1n_1,\ x_2 = h_2n_2$ for some $h_1, h_2 \in H$ and $n_1, n_2 \in N$. Then,

$$\begin{aligned} x_1x_2^{-1} &= h_1n_1n_2^{-1}h_2^{-1} = h_1n_3h_2^{-1} \text{ where } n_3 = n_1n_2^{-1} \in N \\ &= h_1h_2^{-1}h_2n_3h_2^{-1} \text{ where we have inserted } h_2^{-1}h_2 = e \\ &= hn_4 \text{ where } h_1h_2^{-1} = h \in H \text{ and } h_2n_3h_2^{-1} = n_4 \in N \text{ since } N \triangleleft G. \end{aligned}$$

Hence $x_1x_2^{-1} \in HN$ and we conclude HN is a subgroup of G.

c. Show $H/(H \cap N) \cong HN/N$.
We will use the First Isomorphism Theorem 33 found on page 73 for which we need a homomorphism.
Note $HN/N = \{hnN \mid hn \in HN\}$.

But[4] $nN = N$, hence $HN/N = \{hN \mid hn \in HN\}$.
So we can define,

$$\phi : H \to HN/N \text{ by } \phi(h) = hN.$$

Then ϕ is onto since for every $hN \in HN/N$ there is an $h \in H$. Hence recalling Note 15 on page 74, $\phi(H) = HN/N$.
Also ϕ is one-to-one since $\phi(g) = \phi(h) \Rightarrow gN = hN \Rightarrow g = h$.
And ϕ is a homomorphism since, using Definition 32, (coset multiplication, page 68),

$$\phi(h_1h_2) = (h_1h_2)N = (h_1N)(h_2N) = \phi(h_1)\phi(h_2)$$

Now $ker(\phi) = \{x \mid x \in H,\ \phi(x) = e\}$.
But $\phi(x) = e$ means $xN = e$ where $xN = \{xn \text{ for all } n \in N\}$.
So $ker(\phi)$ is the set of x such that $xn = e$ for some $n \in N$.
But only $xx^{-1} = e$, so therefore we must have $x^{-1} \in N$.
But N is a group so we must also have $x \in N$.
Therefore, $ker(\phi) = \{x \mid x \in H \text{ and } x \in N\} = H \cap N$. By the First Homomorphism Theorem 33 on page 73, making the replacements in
$G_1/K \cong \phi(G_1)$ of,

$$\begin{aligned} G_1 &= H, \\ \phi(G_1) &= HN/N, \\ K = ker(\phi) &= H \cap N, \end{aligned}$$

we find,

$$HN/N \cong H/(H \cap N.$$

□

Theorem 35. **** (Third Isomorphism Theorem)*
If N, M are normal subgroups of a group G and M is a subgroup of N, that is we have $N, M \lhd G,\ M \leq N$, then,

$$G/N \cong (G/M)/(N/M)$$

Proof. Noting $G/M = \{aM \mid a \in G\}$, let,

$$\phi : G \to (G/M)/(N/M) \text{ where } \phi(a) = (aM)(N/M) \text{ for all } a \in G.$$

Clearly ϕ is onto, since given any $(aM)(N/M) \in (G/M)/(N/M)$, we have an $a \in G$ so, recalling Note 15, page 74,

$$\phi(G) = (G/M)(N/M).$$

[4] As shown in Note 13 on page 74

And ϕ is one-to-one since $\phi(a) = \phi(b) \Rightarrow (aM)(N/M) = (bM)(N/M) \Rightarrow a = b$.
Also ϕ is a homomorphism, since for all $a, b \in G$ we have,

$$\begin{aligned}\phi(ab) &= [(ab)M](N/M)\\ &= [(aM)(bM)](N/M) \text{ using coset multiplication}\\ &= [(aM)(N/M)][(bM)(N/M)], \text{using coset multiplication}\\ &= \phi(a)\phi(b)\end{aligned}$$

The identity element of $(G/M)/(N/M) = \{(aM)(N/M) \mid a \in G\}$ when multiplied by $(aM)(N/M)$ must leave $(aM)(N/M)$ unchanged. But,

$$\begin{aligned}(aM)(N/M)(N/M) &= (aM)\{n_1Mn_2M \mid n_1, n_2 \in N\}\\ &= (aM)\{n_3M \mid n_3 \in N\},\ n_3 = n_1n_2\\ &= (aM)(N/M)\end{aligned}$$

so (N/M) is the identity element.
Therefore the kernel of ϕ is $\{x \in G \mid \phi(x) = N/M\}$
Since $N/M = \{nM \mid n \in N\}$, it will always be the case that

$$\phi(x) = (xM)(N/M) = N/M$$

provided $x \in N$, say $x = n \in N$, since then,

$$(xM)(N/M) = (nM)(N/M) = (N/M)(N/M) = N/M.$$

But that means $ker(\phi) = N$.
By Theorem 33 on page 73, we have in $G_1/K \cong \phi(G_1)$ using the replacements,

$$\begin{aligned}G &= G_1,\\ \phi(G) &= (G/M)/(N/M),\\ ker(\phi) &= N,\end{aligned}$$

that,

$$G/N \cong (G/M)/(N/M)$$

□

5.7 Key Results

We prove a key result for proving the Insolvability of Polynomials of degree ≥ 5. Specifically we prove in Theorem 36 there is an isomorphism $\phi : S_n \to \mathbb{Z}_2$ with kernel A_n and, using the first isomorphism theorem, Theorem 33, that,

$$S_n/A_n \cong \mathbb{Z}_2, \text{ where } \mathbb{Z}_2 = \{0, 1\}$$

This is a key result we will need to achieve our final result, specifically that S_n/A_n is abelian since it is isomorphic to $\mathbb{Z}_2$ which is obviously abelian.

Theorem 36. *****
The factor group S_n/A_n is isomorphic to $\mathbb{Z}_2 = \{0, 1\}$, that is,

$$S_n/A_n \cong \mathbb{Z}_2$$

Proof. Recall for A_n a subgroup of S_n that for $\phi \in S_n$, a left coset ϕA_n of A_n is given by,

$$\phi A_n = \{\phi\tau \mid \tau \in A_n\}$$

and that the factor group S_n/A_n is defined as the group of cosets,

$$S_n/A_n = \{\phi A_n \mid \phi \in S_n\}$$

Now if $\phi \in A_n$ then ϕA_n is still in the set of all even permutations, so $\phi A_n \in A_n$, and if $\phi \notin A_n$, then ϕA_n is an odd permutation. Since we proved in Theorem 12, page 48, there are an equal number of even and odd permutations, specifically, $|A_n| = \dfrac{|S_n|}{2}$, there are only two cosets, the sets of even and odd permutations. Looking for an isomorphism, we define a function,

$$\psi : S_n/A_n \to \mathbb{Z}_2 \text{ by } \psi(\phi A_n) = \begin{cases} 0, & \text{if } \phi \in A_n \\ 1, & \text{if } \phi \notin A_n \end{cases}$$

Since we are mapping two objects onto two numbers, this mapping is clearly a one-to-one correspondence. We need to prove it is a homomorphism also, that is, with the operation addition mod 2,

$$\psi(\phi_1 A_n \circ \phi_2 A_n) = \psi(\phi_1 A_n) + \psi(\phi_2 A_n)$$

Clearly the composition of two even or two odd permutations is even and the composition of an odd and an even permutation is odd. Under addition modulo 2, there are just four cases to consider.

Case 1: $\phi_1 \in A_n,\ \phi_2 \in A_n \Rightarrow \phi_1 \circ \phi_2 \in A_n$
Then $\psi(\phi_1 A_n \circ \phi_2 A_n) = 0$ and $\psi(\phi_1 A_n) + \psi(\phi_2 A_n) = 0 + 0 = 0$

Case 2: $\phi_1 \in A_n,\ \phi_2 \notin A_n \Rightarrow \phi_1 \circ \phi_2 \notin A_n$
Then $\psi(\phi_1 A_n \circ \phi_2 A_n) = 1$ and $\psi(\phi_1 A_n) + \psi(\phi_2 A_n) = 0 + 1 = 1$

Case 3: $\phi_1 \notin A_n,\ \phi_2 \in A_n \Rightarrow \phi_1 \circ \phi_2 \notin A_n$
Then $\psi(\phi_1 A_n \circ \phi_2 A_n) = 1$ and $\psi(\phi_1 A_n) + \psi(\phi_2 A_n) = 1 + 0 = 1$

Case 4: $\phi_1 \notin A_n,\ \phi_2 \notin A_n \Rightarrow \phi_1 \circ \phi_2 \in A_n$
Then $\psi(\phi_1 A_n \circ \phi_2 A_n) = 0$ and $\psi(\phi_1 A_n) + \psi(\phi_2 A_n) = 1 + 1 = 0$.

Therefore in each case $\psi(\phi_1 A_n \circ \phi_2 A_n) = \psi(\phi_1 A_n) + \psi(\phi_2 A_n)$, so ψ is an isomorphism and $S_n/A_n \cong \mathbb{Z}_2$. □

Chapter 6

Group Theory Part V

Simple and Solvable Groups

Our final chapter on groups concerns simple and solvable groups. Both concepts are an integral part of our proof of the insolvability by radicals of polynomials of degree ≥ 5.

6.1 Simple Groups

Definition 35. *simple group*
A simple group has no normal subgroups other than itself and the identity set $\{e\}$ *which are called the trivial normal subgroups*[1].

We prove in Theorem 38 preceded by Theorem 37 that the subgroups A_n of the symmetric groups S_n are simple groups for $n \geq 5$.

Theorem 37. *****

1. *A_n contains all possible three cycles.*

2. *If $n \geq 5$, no proper normal subgroup of A_n contains a 3-cycle, that is, if any normal subgroup N of A_n contains a 3-cycle, then $N = A_n$.*

Proof. 1. We want to show A_n contains all possible three cycles.
By definition any element of A_n is a product of an even number of 2-cycles. The pairs of 2-cycles can have only the following three forms,

$$\begin{aligned}(a,b)(a,b) &= \text{ the identity}\\ (a,b)(b,c) &= (a,b,c)\\ (a,b)(c,d) &= (a,b,c)(b,c,d)\end{aligned}$$

[1]We proved the trivial subgroups are normal in Theorem 30, page 69.

Thus,

$$A_n = \{id, (r,s,k) \mid 1 \le r,s,k \le n,\ r \ne s,\ k \ne r,\ k \ne s\}$$

or A_n contains all possible three cycles.

2. We want to show if $n \ge 5$, no proper normal subgroup of A_n contains a 3-cycle, that is, if any normal subgroup N of A_n contains a 3-cycle, then $N = A_n$.
Now $N \lhd A_n \Rightarrow N \subseteq A_n$. Let N contain a 3-cycle. We will show $A_n \subseteq N$ so that, by double containment, we must have $N = A_n$.
So suppose $(r,s,c) \in N$. Then, since N is a group, $(r,s,c)^2 \in N$.
Let $\tau = (r,s,c)^2$.
Now $\sigma = (r,s)(c,k) \in A_n$ and hence $\sigma^{-1} = (k,c)(s,r) \in A_n$.
By Definition 31, page 65, of N as a normal group,

$$\begin{aligned} &\tau\sigma\tau^{-1} \in N \ \textit{for all}\ \sigma \in N \ \textit{and}\ \tau \in A_n \\ &\quad \Rightarrow (r,s)(c,k)(r,s,c)^2(k,c)(s,r) \in N \\ &\quad \Rightarrow (r,s,k) \in N \quad \text{(the multiplication is left to the reader)} \end{aligned}$$

Now, by part (1) of this theorem, A_n contains all the 3-cycles, hence $A_n \subseteq N$.
But we noted above that $N \subseteq A_n$. By double containment, $N = A_n$.

□

Theorem 38. *****
The alternating subgroups A_n of the symmetric groups S_n are simple, that is have no non-trivial subgroups, if $n \ge 5$.

Proof. Let N be a normal subgroup of A_n. We want to show we can only have $N = A_n$.
By Theorem 37 (2) we only need to show N contains a 3-cycle.
Let $\sigma \in N$ and assume σ is written as a product of disjoint cycles. The possible cases are:
Case 1: σ is a 3-cycle, then we are done.

Case 2: σ contains a cycle of length ≥ 4, say $(a,b,c,d,\ldots)$.
Let $\tau = (b,c,d) \in A_n$. (remember, by Theorem 37(1), A_n contains all the 3-cycles.)
We will use the following argument in each of the following cases. Since N is a normal subgroup of A_n and $\sigma \in N$, both σ^{-1} and $\tau\sigma\tau^{-1}$ (by definition of a normal subgroup) belong to N.
In this Case 2, therefore their product,

$$\sigma^{-1}\tau\sigma\tau^{-1} = (\ldots,d,c,b,a)(b,c,d)(a,b,c,d,\ldots)(d,c,b) = (a,b,d) \in N$$

and we again have $N = A_n$ since N contains a 3–cycle.

Case 3: σ contains a 3-cycle but no longer cycle. We have two possibilities.

Case 3A: $\sigma = (a,b,c)(d,f,g)\ldots.$
Again, let $\tau = (b,c,d) \in A_n$ and compute,

$$\sigma^{-1}\tau\sigma\tau^{-1} = \ldots(g,f,d)(c,b,a)(b,c,d)(a,b,c)(d,f,g)(d,c,b)\ldots = (a,b,d,c,g) \in N$$

This is a cycle of length greater than 4 so by Case 2 we again have $N = A_n$.

Case 3B: $\sigma = (a,b,c)(d,f)\ldots.$
Then, with $\tau = (b,c,d)$,

$$\sigma^{-1}\tau\sigma\tau^{-1} = (f,d)(c,b,a)(b,c,d)(a,b,c)(d,f)(d,c,b)\ldots = (a,b,d,c,f) \in N$$

Again, this is a cycle of length greater than 4 so by Case 2 we have $N = A_n$.

Case 4: σ contains only 2-cycles. There are two possibilities.
Case 4A: $\sigma = (a,b)(c,d)$
Let $\mu = (c,d,e) \in A_n$ and compute,

$$\sigma^{-1}\mu\sigma\mu^{-1} = (d,c)(b,a)(c,d,e)(a,b)(c,d)(e,d,c) = (c,d,e) \in N$$

We conclude $N = A_n$.

Case 4B: $\sigma = (a,b)(c,d)\ldots.$
Let $\tau = (b,c,d) \in A_n$ and compute,

$$\sigma^{-1}\tau\sigma\tau^{-1} = \ldots(d,c)(b,a)(b,c,d)(a,b)(c,d)(d,c,b)\ldots = (a,d)(b,c),$$

which is Case 4A so again $N = A_n$.
There are no other possibilities so A_n is simple. □

We then prove in Theorem 39 that the subgroups $A_n,\ n \geq 5$ are not abelian groups (see Definition 6) for $n \geq 5$, again a vital result for achieving our major goal.

Theorem 39. *
A_n is not abelian for $n \geq 5$.

Proof. We only need one counter example, so this will suffice. Again, note A_n contains all the 3-cycles.

$$(1,2,3)(3,4,5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & \ldots \\ 2 & 3 & 1 & 4 & 5 & 6 & \ldots \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & \ldots \\ 1 & 2 & 4 & 5 & 3 & 6 & \ldots \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & \ldots \\ 2 & 3 & 4 & 5 & 1 & 6 & \ldots \end{pmatrix}$$

$$(3,4,5)(1,2,3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & ... \\ 1 & 2 & 4 & 5 & 3 & 6 & ... \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & ... \\ 2 & 3 & 1 & 4 & 5 & 6 & ... \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & ... \\ 2 & 4 & 1 & 5 & 3 & 6 & ... \end{pmatrix}$$

Hence $(1,2,3)(3,4,5) \neq (3,4,5)(1,2,3)$ so A_n is not an abelian subgroup of the symmetric group S_n for $n \geq 5$. □

You may choose to investigate some $n < 5$ cases and later relate these findings back to the fact that polynomials of degree less than 5 are solvable by radicals as we found in Chapter 2.

6.2 Subnormal Series

Definition 36. *subnormal series*
A subnormal series of a group is a finite chain of subgroups,

$$\{e\} = G_0 \leq G_1 \leq G_2 \leq \ldots \leq G_n = G$$

such that $G_i \triangleleft G_{i+1}$ for all i such that $1 \leq i \leq n-1$, that is G_i is a normal subgroup of G_{i+1}.

The key result we will be using is that we have the subnormal series,

$$\{e\} = \{\rho_0\} \ < \ A_n \ < \ S_n$$

where ρ_0 is the identity permutation. This is true since $\{e\} \triangleleft A_n$ by Theorem 24, page 65, and $A_n \triangleleft S_n$ by Theorem 29, page 68.

We need to extend the definition of a subnormal series as follows. The use of the word "solvable" indicates that we are heading in the direction of the solvability of polynomials by radicals.

6.3 Solvable Groups

Definition 37. *solvable group*
A group G is solvable if it has a subnormal series such that the factor groups G_{i+1}/G_i are abelian, that is, we can form a finite chain of subgroups,

$$\{e\} = G_0 \leq G_1 \leq G_2 \leq \ldots \leq G_n = G$$

such that $G_i \triangleleft G_{i+1}$ and the factor groups G_{i+1}/G_i are all abelian for $1 \leq i \leq n-1$.

Example 39. *For example, S_3 is solvable since the subnormal series,*

$$\{e\} = \{\rho_0\} \ < \ A_3 \ < \ S_3$$

has factor groups $S_3/A_3 \cong \mathbb{Z}_2,\ A_3/\{\rho_0\} \cong \mathbb{Z}_3$, (See Theorem 36, page 78 for the first, the second isomorphism is left to the reader), both of which are abelian and $\{e\} \lhd A_3$, (Theorem 24, page 65) and $A_3 \lhd S_3$ (Theorem 29, page 68). ⋄

It can be shown in a similar manner that S_4 is also solvable. What we need is Theorem 40 that $S_n, n \geq 5$ is not solvable since the subnormal series,

$$\{\rho_0\} \ < \ A_n \ < \ S_n$$

has an abelian factor group $S_n/A_n \cong \mathbb{Z}_2$, but the other factor group is $A_n/\{\rho_0\} \cong A_n$ which, by Theorem 39, is NOT abelian for $n \geq 5$.

Theorem 40. ***
The symmetric groups, $S_n, n \geq 5$ are not solvable.

Proof. The subnormal series,

$$\{e\} = \{\rho_0\} \ < \ A_n \ < \ S_n$$

has the factor group S_n/A_n which, by Theorem 36, page 78, is isomorphic to $\mathbb{Z}_2 = \{0, 1\}$ which is obviously abelian but also the factor group $A_n/\{\rho_0\}$. But,

$$A_n/\{\rho_0\} = \{\rho_0\tau \mid \tau \in a_n\} = \{\tau \mid \tau \in A_n\} = A_n,$$

which is not abelian by Theorem 39, page 81, so we do not have a solvable group. □

Note 16. *It is the fact that $S_n, n \geq 5$ is not solvable that was used by Galois to prove the insolvability by radicals of polynomials of degree ≥ 5 and, further, to enable us to actually find some examples of such polynomials. An obvious question is whether S_n can have other series which may have abelian factor groups. That was answered for all groups in the negative by the Jordan Holder theorem. But we only need Theorem 41, that for $n \geq 5,\ A_n$ is the only proper nontrivial normal subgroup of S_n.*

Theorem 41. *****
For $n \geq 5,\ A_n$ is the only proper nontrivial normal subgroup of S_n.

Proof. Let $N \trianglelefteq S_n$ be normal. We want to show $N = \{e\}$ which is trivial, or $N = S_n$ which is also trivial, or $N = A_n$.

*****

We first prove $N \cap A_n \trianglelefteq A_n$.
Since $N \trianglelefteq S_n$ then $\alpha\beta\alpha^{-1} \in N$ for all $\alpha \in S_n$ and $\beta \in N$.
Now if $\alpha\beta\alpha^{-1} \in N$ for all $\alpha \in S_n$ and $A_n \subset S_n$ then $\alpha\beta\alpha^{-1} \in N$ for all $\alpha \in A_n$.
Now obviously a subgroup N of S_n cannot contain only odd permutations else we do not have closure since in N we have the product of an odd permutation by itself which is an even permutation. Hence there is an even permutation $\beta \in N$ and, of course, we also have $\beta \in A_n$.
But A_n is a group (see Theorem 11, page 47) so if $\beta \in A_n$ and $\alpha \in A_n$ then $\alpha\beta\alpha^{-1} \in A_n$ for all $\alpha \in A_n$ and $\beta \in N \cap A_n$.
Thus $\alpha\beta\alpha^{-1} \in A_n$ as well as $\alpha\beta\alpha^{-1} \in N$ so $\alpha\beta\alpha^{-1} \in N \cap A_n$ for all $\alpha \in A_n$ and $\beta \in N \cap A_n$.
Then, by Definition 26, page 55, $N \cap A_n \trianglelefteq A_n$ as we wished to prove.

*****

We proceed to prove that for $n \geq 5$, A_n is the only proper normal subgroup of S_n.
By Theorem 38, page 80, A_n is simple and can have no normal non-trivial subgroups, so if $N \cap A_n \trianglelefteq A_n$ as we just proved, then we have two possibilities, $N \cap A_n = A_n$ or $N \cap A_n = \{e\}$.
In the first case, if $N \cap A_n = A_n$, then either $N = A_n$ or $N = S_n$, which is trivial.
In the second case, if $N \cap A_n = \{e\}$, then either $N = \{e\}$ or else N consists solely of one or more odd permutations in addition to the identity element $\{e\}$.
But N cannot consist of more than one odd permutation since if N contains two distinct odd permutations, σ and τ, then N also has the elements σ^2 and $\sigma\tau$, not both of which can be the identity e. But both σ^2 and $\sigma\tau$ are even, contradicting the assumption that N contains only odd nontrivial permutations.
Thus N can consist only of the elements σ, e where σ is the single odd permutation. But then N also contains σ^2 which must equal e so N has order 2.
Then such a subgroup cannot be normal for this reason. Suppose an odd permutation of order 2 has as its cycle decomposition an odd number, one or more, of disjoint 2-cycles[2]. Then suppose without loss of generality that $\sigma = (1, 2)$ is one of these 2-cycles. Let $\tau = (1, 3) \in S_n$. Then we should have $\tau\sigma\tau^{-1} \in N$ since $N \trianglelefteq S_n$, but,

$$\tau\sigma\tau^{-1} = (1, 3)(1, 2)(3, 1)$$

takes 2 to 3 and thus is neither $\sigma = (1, 2)$ which takes 2 to 1 nor e which takes 2 to 2. So this group is not normal in S_n since that would require $\tau\sigma\tau^{-1} \in N = \{e, \sigma\}$.
We conclude for $n \geq 5$ that A_n is the only proper nontrivial normal subgroup of S_n. □

Before we conclude this discussion of groups we prove in Theorem 42 that subgroups and factor groups of solvable groups are also solvable, results we need in our ultimate proofs, albeit this (very long) proof is quite demanding. You may prefer to just browse this proof at first reading.

[2]By Theorem 10, page 47, every cycle can be written as the product of 2–cycles.

Theorem 42. *******
Let G be a solvable group. Then,

(a) Any subgroup of G is solvable.

(b) If N is a normal subgroup of G then the factor group G/N is solvable.

Proof. Let G be a solvable group. Then by Definition 44, page 94, we have the subnormal series,

$$\{e\} = H_0 \subseteq H_1 \subseteq \ldots \subseteq H_n = G$$

of G with H_{i+1}/H_i abelian and $H_i \trianglelefteq H_{i+1}$ for $1 \leq i \leq n-1$.

*****

Proof of (a) We will show that if K is a subgroup of G then,

$$\{e\} = K \cap H_0 \subseteq K \cap H_1 \subseteq \ldots K \cap H_n = K$$

is a subnormal series with $K \cap H_{i+1}/K \cap H_i$ abelian and $K \cap H_i \trianglelefteq K \cap H_{i+1}$, so that, by definition, K is solvable.
Now since, $H_i \cap H_{i+1} = H_i$, we have both,

$$K \cap H_i = \big(K \cap H_{i+1}\big) \cap H_i,\ 0 \leq i \leq n-1,\ \text{and,}$$
$$K \cap H_n = K \cap G = K.$$

Further, by Definition 37 on page 82 of a subnormal series, $H_i \trianglelefteq H_{i+1}$.
We also have $K \cap H_{i+1}$ is a subgroup[3] of H_{i+1}.
The Second Isomorphism Theorem 34, page 75 states that if N is a normal subgroup of a group G and H is a subgroup of G then,

(i) $H \cap N \trianglelefteq H$

(ii) HN is a subgroup of G

(iii) $H/H \cap N \cong HN/N$

We make the replacements,

- $G \leftrightarrow H_{i+1}$
- $H \leftrightarrow K \cap H_{i+1}$
- $N \leftrightarrow H_i$

[3]In general, if A and B are subgroups of a group G, then $A \cap B$ is a subgroup of either A or B. The reason is that if $b \in A \cap B$ then $b \in A$ and $b \in B$. But A and B are groups and therefore $b^{-1} \in A$ and $b^{-1} \in B$ so $b^{-1} \in A \cap B$. Then if also $a \in A \cap B$ then $ab^{-1} \in A \cap B$ making $A \cap B$ a subgroup of A by Corollary 3, page 31. Similarly $A \cap B$ is a subgroup of B.

for the group H_{i+1} with subgroup $K \cap H_{i+1}$ and normal subgroup H_i to obtain from (i) and (iii),

$$(K \cap H_{i+1}) \cap H_i \lhd K \cap H_{i+1} \tag{6.3.1}$$
$$(K \cap H_{i+1})/((K \cap H_{i+1}) \cap H_i) \cong ((K \cap H_{i+1})H_i)/H_i \tag{6.3.2}$$

Since $H_i \cap H_{i+1} = H_i$ and $(K \cap H_{i+1}) \cap H_i = K \cap H_i$, it follows from (6.3.1) and (6.3.2) that,

$$(K \cap H_i) \lhd K \cap H_{i+1} \tag{6.3.3}$$
$$(K \cap H_{i+1})/(K \cap H_i) \cong ((K \cap H_{i+1})H_i)/H_i \tag{6.3.4}$$

Equation (6.3.3) gives us a chain of subgroups each normal in the next. We need to show the factor groups are abelian to prove we have a solvable group.

***

First, we claim $(K \cap H_{i+1})H_i \subseteq H_{i+1}$. To prove the claim we need to show if $x \in K \cap H_{i+1}$ and $y \in H_i$ then $xy \in H_{i+1}$.
But if $x \in K \cap H_{i+1}$ then $x \in H_{i+1}$ and if $y \in H_i$ then $y \in H_{i+1}$ since $H_i \subset H_{i+1}$. Hence $xy \in H_{i+1}$ since H_{i+1} is a group, proving $(K \cap H_{i+1})H_i \subseteq H_{i+1}$.

*****

Now, in general, it is a fact that if we have groups A, B, C such that $A \subset B$ then $A/C \subset B/C$.
The reason for this is if $A \subset B$, then any $a \in A$ is also in B, say $a = b \in B$.
Then if $aC \in A/C = \{aC \mid a \in A\}$ then $aC = bC$ for some $b \in B$ and then
$aC \in \{bC \mid b \in B\} = B/C$. We conclude $A/C \subset B/C$.

*****

It therefore follows, that since $(K \cap H_{i+1})H_i \subseteq H_{i+1}$ by the claim proved above, we must have,

$$(K \cap H_{i+1})H_i/H_i \subseteq H_{i+1}/H_i.$$

But H_{i+1}/H_i is abelian by assumption and hence so is (a subgroup) $(K \cap H_{i+1})H_i/H_i$ and therefore, by Theorem 20 on page 58 and (6.3.4), its isomorphic group $(K \cap H_{i+1})/(K \cap H_i)$ is also abelian. We conclude,

$$\{e\} = K \cap H_0 \subseteq K \cap H_1 \subseteq \ldots K \cap H_n = K$$

is a subnormal series with $K \cap H_{i+1}/K \cap H_i$ abelian and $K \cap H_i \lhd K \cap H_{i+1}$, so that, by definition, K is solvable.

****

Proof of (b) We will show if N is a normal subgroup of the solvable group G then the factor group G/N is solvable.
Let G have the subnormal series,

$$\{e\} = H_0 \subseteq H_1 \subseteq \ldots \subseteq H_n = G$$

where $H_i \lhd H_{i+1}$ and H_{i+1}/H_i are abelian.
Consider the homomorphism[4] $\phi : G \to G/N$ where every subgroup of G is mapped by ϕ onto a subgroup of G/N. In particular, let $\tilde{H}_i = \phi(H_i)$.
First we will prove $\tilde{H}_i \lhd \tilde{H_{i+1}}$ but first we need to prove two claims.

*****

Claim 1
If $\theta : G \to K$ is a homomorphism and H is a subgroup of G then $\theta(H)$ is a subgroup of K. And if H is a normal subgroup of G, that is $H \lhd G$, then $\theta(H)$ is a normal subgroup of K.
Proof of Claim 1
If $x_1,\ x_2 \in \theta(H)$ such that $x_1 = \theta(h_1),\ x_2 = \theta(h_2)$, for some $h_1, h_2 \in H$, then

$$x_1 x_2^{-1} = \theta(h_1)\theta(h_2)^{-1} = \theta(h_1)\theta(h_2^{-1}) = \theta(h_1 h_2^{-1}) = \theta(h) \in \theta(H))$$

where $h = h_1 h_2^{-1}$. Hence, by the subgroup test (Corollary 3, page 31), $\theta(H)$ is a subgroup of K.

*****

Second, to prove $H \lhd G \Rightarrow \phi(H) \lhd K$ we need to show,

$$\theta(g)\theta(h)\theta(g^{-1}) \in \theta(H) \ \textit{for all}\ \theta(g) \in K \ \textit{and}\ \theta(h) \in \theta(H).$$

If now $H \lhd G$, then by Definition 31 on page 65, $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$.
Now any element $k \in K$ is of the form $\theta(g)$ for some $g \in G$ and any element of $\theta(H)$ is of the form $\theta(h)$ for some $h \in H$.
Since θ is a homomorphism,

$$\theta(g)\theta(h)\theta(g)^{-1} = \theta(ghg^{-1}).$$

But since $ghg^{-1} \in H$, we have,

$$\theta(ghg^{-1}) \in \theta(H) \Rightarrow \theta(g)\theta(h)\theta(g)^{-1} \in \theta(H)$$

for all $\theta(g) \in K$ and $\theta(h) \in \theta(H)$.
Hence, by Definition 31, $\theta(H) \lhd K$ or $\theta(H)$ is a normal subgroup of K. This proves Claim 1.

[4] If $\phi(g) = gN,\ \phi(h) = hN$ then $\phi(gh) = ghN = gNhN = \phi(g)\phi(h)$, so ϕ is a homomorphism.

*****

Claim 2
If N is a normal subgroup of G and H is any subgroup of G then $H \cap N$ is a normal subgroup of H. That is, if $N \lhd G$ and $H < G$ then $H \cap N \lhd H$.
Proof of Claim 2
We use Definition 31 on page 65 of a normal subgroup repeatedly.
We need to show $hkh^{-1} \in H \cap N$ for all $h \in H$ and $k \in H \cap N$.
We are given $N \lhd G$ so $gng^{-1} \in N$ for all $g \in G$ and $n \in N$.
Now, if $h \in H \subset G$ then $h \in G$.
So, putting $h = g$ we have,

$$hnh^{-1} \in N \text{ for all } h \in H \text{ and } n \in N. \tag{6.3.5}$$

Also if $k \in H \cap N$ then $k \in N$ so, by (6.3.5)

$$hkh^{-1} \in N \text{ for all } h \in H \textit{ and } k \in H \cap N. \tag{6.3.6}$$

Further, if $h \in H$ then $h^{-1} \in H$ and if $k \in H \cap N$ then $k \in H$.
Consequently, since H is a group,

$$hkh^{-1} \in H \text{ for all } h \in H \text{ and } k \in H \cap N. \tag{6.3.7}$$

Hence, by (6.3.6) and (6.3.7),

$$hkh^{-1} \in H \cap N \text{ for all } h \in H \text{ and } k \in H \cap N.$$

This proves $H \cap N \lhd H$, so Claim 2 is proved.

*****

We now proceed to establish the requirements for a subnormal series of G/N.
First we show $\tilde{H}_i \lhd \tilde{H_{i+1}}$ where $\tilde{H}_i = \phi(H_i$.
Define $\phi : H_{i+1} \to H_{i+1}/H_i$ by $\phi(h) = hH_i$ for all $h \in H_{i+1}$. Then ϕ is a homomorphism since $\phi(hk) = hkH_i = hH_ikH_i = \phi(h)\phi(k)$.
So substituting our data into the statement of Claim 1, we have since $H_i \lhd H_{i+1}$ that,

$$\phi(H_i) \lhd H_{i+1}/H_i \Leftrightarrow \tilde{H}_i \lhd H_{i+1}/H_i.$$

With these same replacements, Claim 2 proves if $\tilde{H}_i \lhd H_{i+1}/H_i$ and $\tilde{H_{i+1}} < H_{i+1}/H_i$ (which is true since ϕ maps H_{i+1} into H_{i+1}/H_i), then,

$$\tilde{H}_i \cap \tilde{H_{i+1}} \lhd \tilde{H_{i+1}}$$

But, $\tilde{H}_i \cap \tilde{H_{i+1}} = \tilde{H}_i$, so we have,

$$\tilde{H}_i \lhd \tilde{H_{i+1}}.$$

*****

Second, we claim $\tilde{H_{i+1}}/\tilde{H}_i$ is abelian.
Let $\tilde{x} = \phi(x)$ and $\tilde{y} = \phi(y)$ for any two elements $x, y \in H_{i+1}$.
Note $\tilde{x}\tilde{y} = \phi(x)\phi(y) = \phi(xy)$.
Since,

$$\tilde{H_{i+1}}/\tilde{H}_i = \phi(H_{i+1})/\phi(H_i) = \{\tilde{x}\phi(H_i) \mid \tilde{x} \in \phi(H_{i+1})\} = \{\tilde{x}\tilde{H}_i \mid \tilde{x} \in \tilde{H_{i+1}})\},$$

$\tilde{H_{i+1}}/\tilde{H}_i$ abelian is shown by proving,

$$\tilde{x}\tilde{H}_i\tilde{y}\tilde{H}_i = \tilde{y}\tilde{H}_i\tilde{x}\tilde{H}_i$$

Now, since H_{i+1}/H_i is abelian, we have,

$$\begin{aligned}
&xH_iyH_i = yH_ixH_i \\
&\quad\Rightarrow xyH_i = yxH_i \quad \text{(using coset multiplication, Definition 37, page 82)} \\
&\quad\Rightarrow xyh_1 = yxh_2 \quad \text{for some } h_1, h_2 \in H_i \\
&\quad\Rightarrow xyh_1h_1^{-1} = yxh_2h_1^{-1} \\
&\quad\Rightarrow xy = yxd \quad \text{for some } d \in H_i, \text{ where } d = h_2h_1^{-1}
\end{aligned}$$

Thus,

$$\phi(xy) = \phi(yxd) \Rightarrow \phi(x)\phi(y) = \phi(y)\phi(x)\phi(d) \tag{6.3.8}$$

But $d \in H_i \Rightarrow \phi(d) \in \tilde{H}_i$. Therefore,

$$\phi(d)\tilde{H}_i = \tilde{H}_i \text{ (by } Note \text{ 15 } page \text{ 74)}, \tag{6.3.9}$$

and,

$$\begin{aligned}
\tilde{x}\tilde{H}_i\tilde{y}\tilde{H}_i &= \tilde{x}\tilde{y}\tilde{H}_i \\
&= \phi(x)\phi(y)\tilde{H}_i \\
&= \phi(y)\phi(x)\phi(d)\tilde{H}_i \text{ by (6.3.8)} \\
&= \phi(y)\phi(x)\tilde{H}_i \text{ by (6.3.9)} \\
&= \tilde{y}\tilde{x}\tilde{H}_i \\
&= \tilde{y}\tilde{H}_i\tilde{x}\tilde{H}_i. \text{ by coset multiplication}
\end{aligned}$$

Therefore $\tilde{H}_{i+1}/\tilde{H}_i$ is abelian.

****

Thus, the requirements for a solvable group as set out in Definition 37, page 82 are fully covered and,

$$\{e\} = \tilde{H}_0 \lhd \tilde{H}_1 \lhd \ldots \lhd \tilde{H}_n = G/N$$

is a subnormal series of G/N with abelian factors, and therefore G/N is solvable. □

Chapter 7

Rings and Fields

7.1 Introduction

The second half of our quest involves finding what we will call the Galois groups of polynomials and then relating them to fields formed from the rationals and the roots of the polynomials. We need the algebraic structures called fields and rings. The first abstract algebraic objects we studied were groups. A group is associated with only one binary operation, often either addition or multiplication. Obviously in dealing with these number sets in our normal lives, we employ two binary operations,

- Addition, for example, $\frac{3}{4} + \frac{1}{2} = \frac{5}{4}$
- Multiplication, for example, $6 \times \frac{2}{3} = 4$

You may ask, what about subtraction and division? But they are just addition and multiplication involving inverses.

- Subtraction, for example, $6 - 3 = 6 + (-3) = 3$
- Division, for example, $12 \div 3 = 12 \times 3^{-1} = 12 \times \frac{1}{3} = 4$

So we need more than groups. We proceed in two steps, defining fields and rings.

A field is basically two connected groups. It is a set on which two binary operations, addition and multiplication, are defined and for which the set is an abelian group under addition and the nonzero elements of the set are a group under multiplication. The distributive law $a(b+c) = ab + ac$ also holds.

A ring is "almost" a field. The exception to the field laws is that ring elements may not have multiplicative inverses or a multiplicative identity. Obviously the integers are the classic example, obeying all the rules for a group under addition and multiplication as well as the distributive law, except, with the exception of ± 1, integers do not have multiplicative inverses. For example, the multiplicative inverse of 7 is $\frac{1}{7}$ but this is not an integer.

If the elements of the ring commute under the two operations and if the multiplicative identity 1 is an element of the ring, we classify it as a commutative ring with identity.

Here are the definitions in detail.

7.2 Rings

Definition 38. *rings*
A ring is a set, together with two binary operations, usually $+, \times$, that is an abelian group under addition (closure, associativity, commutativity, identity, inverses) to which we add two more criteria,

- *Multiplication that is associative, that is $(ab)c = a(bc)$ (but no multiplicative identity or inverses or commutativity)*
- *The left and right distributive laws, $a(b+c) = ab + ac$; $(b+c)a = ba + ca$*

Clearly, $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all rings but we are not using their full "power". First they are commutative rings with identity, meaning the elements commute under the operations of $+, \times$ and the multiplicative identity 1 is also an element. But they are also fields.

First, however, let's discuss some facts about rings. Just as for groups, we have homomorphisms and a fundamental theorem.

Definition 39. *ring homomorphism*
Let R, S be commutative rings. A function $\phi : R \to S$ is called a ring homomorphism if for all $a, b \in R$ it is a group homomorphism under the two operations, that is,

$$\phi(a+b) = \phi(a) + \phi(b)$$
$$\phi(ab) = \phi(a)\phi(b)$$

As with groups we note that if $*_R, *_S$ are the respective additive operations for R and S we should, strictly speaking, write $\phi(a *_R b) = \phi(a) *_S \phi(b)$, similarly for multiplication.

Definition 40. *ring isomorphism*
A ring homomorphism that is one-to-one and onto is called a ring isomorphism.

Definition 41. *isomorphic rings*
If there is a ring isomorphism from ring R onto ring S we say R is isomorphic to S and we write $R \cong S$.

As for groups we could prove the theorems for ϕ, R, S as above:

- The inverse of a ring homomorphism is a ring homomorphism.
- The composition of two ring homomorphisms is a ring homomorphism.

- $\phi(e_1) = e_2$
- $\phi(-a) = -\phi(a)$ or $\phi(a^{-1}) = (\phi(a))^{-1}$

Again, as for groups, we define the kernel of a ring homomorphism,

Definition 42. *kernel of a ring homomorphism*
Let $\phi : R \to S$ be a ring homomorphism for rings R, S. The set $\{a \in R \mid \phi(a) = e\}$ is called the kernel of ϕ, written $ker(\phi)$.

We prove two theorems.

Theorem 43. ***
Let $\phi : R \to S$ be a ring homomorphism with kernel $ker(\phi)$. Then $R/ker(\phi)$ is a commutative ring.

Proof. Note that R and S are abelian or commutative by definition. Therefore so is $\phi(R)$ which is contained within S.
First we need to show $R/ker(\phi)$ is an abelian group under addition but that is proved by the Fundamental Homomorphism Theorem 33 on page 73 for groups since $R/ker(\phi)$ is isomorphic to $\phi(R)$ which is abelian since, by definition, R is abelian.
Second, to show $R/ker(\phi)$ is a ring, we need to verify the distributive, associative and commutative laws hold for multiplication. We let $[a], [b]$, etc. be the cosets of $ker(\phi)$ so that $R/ker(\phi) = \{[a], [b], \ldots\}$.
As we discussed in Section 5.4.2 and proved in Theorem 31 on page 70, we have the well-defined operations of addition and multiplication on cosets given by,

$$[a] + [b] = [a + b]$$
$$[a][b] = [ab]$$

Then we have for the distributive, commutative and associative laws respectively, using inside the parentheses the same laws applying to R which is abelian,

$$[a]([b] + [c]) = [a][b + c] = [ab + ac] = [ab] + [ac] = [a][b] + [a][c]$$
$$[a] + [b] = [a + b] = [b + a] = [b] + [a]$$
$$[a] + ([b] + [c]) = [a] + [b + c] = [a + b + c] = [a + b] + [c] = [a] + [b] + [c]$$

Hence $R/Ker(\phi)$ is a commutative ring. □

Theorem 44. *** *(Fundamental Homomorphism Theorem for Rings)*
Let $\phi : R \to S$ be a ring homomorphism with kernel $ker(\phi)$. Then $R/ker(\phi) \cong \phi(R)$.

Proof. Since $\phi : R \to S$ is a group homomorphism under addition, the proof of the Fundamental Homomorphism Theorem 33, page 73, tells us that, with $K = ker(\phi)$, since the map

$$\psi : R/K \to \phi(R), \text{ where } \psi(a + K) = \phi(a)$$

is a group homomorphism[1] then $R/ker(\phi) \cong \phi(R)$.
To show ψ is a ring homomorphism we need to show it preserves multiplication.
Let $a+K,\ b+K \in R/K$. Then,

$$\psi[(a+K)(b+K)] = \psi(ab+K) = \phi(ab) = \phi(a)\phi(b) = \psi(a+K)\psi(b+K).$$

So ψ preserves multiplication making it a ring homomorphism so we have isomorphic rings and not just groups. □

7.3 Fields

Definition 43. *fields*
Fields are sets that are abelian groups under addition and the non-zero elements are an abelian group under multiplication. We also have the distributive laws,

$$a(b+c) = ab+ac;\ (b+c)a = bc+ca$$

Briefly, a field is a ring with multiplicative identity and multiplicative inverses for the set of non-zero elements.

Note that whenever we discuss the multiplicative inverses of $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, we always exclude 0.

Example 40. *An interesting example of a field and one that gives us a taste of what's to come is* $\mathbb{Q}(\sqrt{2})$, *spoken as "* $\mathbb{Q}$ *append* $\sqrt{2}$ *" and defined by,*

$$\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}$$

There are eleven axioms to be confirmed, five for each of the two abelian groups under addition and multiplication and then the distributive law. Let's consider only,

- *Additive identity is* $0 = 0+0\sqrt{2}$
- *Additive inverse of* $a+b\sqrt{2}$ *is* $-a-b\sqrt{2}$. *Thus,*

$$(a+b\sqrt{2}) + (-a-b\sqrt{2}) = (a-a) + (b-b)\sqrt{2} = 0$$

- *Multiplicative identity is* $1 = 1+0\sqrt{2}$.
- *Multiplicative inverse of* $a+b\sqrt{2}$ *is* $\dfrac{a}{a^2-2b^2} - \dfrac{b}{a^2-2b^2}\sqrt{2}$. *Thus,*

$$(a+b\sqrt{2})\left(\frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}\right) = \frac{a^2-2b^2}{a^2-2b^2} = 1$$

[1] Observe $\psi(a+K+b+K) = \psi(a+b+K) = \phi(a+b) = \phi(a)+\phi(b) = \psi(a+K)+\psi(b+K)$.

Note, given $a, b \in \mathbb{Q}$ *so that* $\frac{a}{b} \in \mathbb{Q}$, *then,* $a^2 - 2b^2 \neq 0$ *since* $a^2 - 2b^2 = 0$ *would mean* $\frac{a}{b} = \sqrt{2}$ *which is not an element of* $\mathbb{Q}$. $\diamond$

Here is the full set of field axioms.

Let F be a set on which two binary operations called addition $(+)$ and multiplication $(\cdot)$ are defined. Then F is called a field if the following properties hold.

1. Closure of F under addition and multiplication:
   For all $a, b \in F$ both $a + b$ and $a \cdot b$ are in F.

2. Associativity of addition and multiplication:
   For all $a, b, c \in F$ the following equalities hold:
   $a + (b + c) = (a + b) + c;\ a \cdot (b \cdot c) = (a \cdot b) \cdot c$

3. Commutativity of addition and multiplication:
   For all $a, b \in F$, the following equalities hold:
   $a + b = b + a;\ a \cdot b = b \cdot a$

4. Existence of additive and multiplicative identity elements:
   There exists an element of F called the additive identity element and denoted by 0 such that for all $a \in F,\ a + 0 = 0 + a = a$
   Likewise, there is an element called the multiplicative identity element and denoted by 1 such that for all $a \in F,\ a \cdot 1 = 1 \cdot a = a$

5. Existence of additive inverses and multiplicative inverses:
   For every $a \in F$, there exists an additive identity element $-a \in F$ such that $a + (-a) = 0$.
   Similarly, for any $a \in F$ other than 0, there exists an multiplicative identity element $a^{-1} \in F$ such that $a \cdot a^{-1} = 1$.
   (The expressions $a + (-b)$ and $a \cdot b^{-1}$ are also denoted $a - b$ and a/b, respectively. In other words, subtraction and division operations exist.)

6. Distributivity of multiplication over addition:
   For all $a, b, c \in F$, the following equality holds: $a \cdot (b + c) = a \cdot b + a \cdot c$.

Note that the requirement for two binary operations means we need to extend the definition of an isomorphism between fields just as we did for ring homomorphisms.

Definition 44. *field isomorphism*
An field isomorphism between fields F, K *is a one-to-one and onto function (a one-to-one correspondence)* $\phi : K \to F$ *such that for all* $a, b \in K$,

$$\phi(ab) = \phi(a)\phi(b)$$
$$\phi(a + b) = \phi(a) + \phi(b)$$

Given the axioms, we can now prove theorems which seem simple since you know them to be true for real and complex numbers (omitting 0), but they are now also true for the infinity of fields in general, for example $\mathbb{Q}(\sqrt{3})$ with $0 = 0 + 0\sqrt{3}$ deleted.

Theorem 45. ***
Let F be a field with elements a, b, c. Then we have,

(a) Cancellation law: $a + c = b + c \Rightarrow a = b$, and $ac = bc \Rightarrow a = b$.

(b) Uniqueness of identity elements: $a + b = a \Rightarrow b = 0$ and $ac = a \Rightarrow c = 1$, provided $a \neq 0$.

(c) Uniqueness of inverses: $a + b = 0 \Rightarrow b = -a$, and if $a \neq 0$, then $ab = 1 \Rightarrow b = a^{-1}$.

Proof. We can prove (a) and (b) and (c) together.
F is a group under both addition and multiplication – we already have these properties for groups. □

Theorem 46. ***
Let F be a field and $a, b \in F$. Then,

(a) $a \cdot 0 = 0$.

(b) If $a \neq 0,\ b \neq 0$ then $ab \neq 0$.

(c) $-(-a) = a$.

(d) $(a)(-b) = (-a)(b) = -ab$

(e) $(-a)(-b) = ab$.

Proof. The proofs are straightforward.

(a) $a \cdot 0 + a \cdot 0 = a(0 + 0) = a \cdot 0 = a \cdot 0 + 0$ and use cancellation.

(b) We use a contrapositive proof to show if $a \cdot b = 0$ then $a = 0$ or $b = 0$. So let $a \cdot b = 0$ and suppose $a \neq 0$. Then by (a), $a \cdot b = 0 = a \cdot 0$ and by cancellation, $b = 0$.

(c) We have both $(-a) - (-a) = 0$ and $(-a) + a = 0$ so $(-a) - (-a) = (-a) + a$. Use cancellation.

(d) We have both $ab + a(-b) = a(b + (-b)) = a \cdot 0 = 0$ and $ab + (-ab) = 0$ so that $ab + a(-b) = ab + (-ab)$ and use cancellation.
Similarly, $(-a)(b) = -ab$.

(e) We have,

$$\begin{aligned}(-a)(-b) &= -(-a)(b) \text{ by (d)} \\ &= -(-ab) \text{ by (d)} \\ &= ab \text{ by (c)}\end{aligned}$$

□

7.4 Finite Cyclic Groups

We now want to prove the theorem that if F is a finite field with multiplicative group $F^\times$ then $F^\times$ is a cyclic group. We need some results for integers proved in Chapter 8, they do not depend on anything we proceed to prove in Section 7.4. We begin with a definition.

Definition 45. *exponent of a group*
Let G be a finite group. The exponent of G, denoted $exp(G)$, is the least common multiple[2] of the orders of all the elements of G. That means if there are integers n such that $a^n = e$ for all $a \in G$, then the least positive value of n is the exponent of G.

Example 41. *The orders of elements of S_3 are 1, 2, 3 as shown below. We have $lcm(1,2,3) = 6$, so $exp(S_3) = 6$.*

$$Order\ 1: \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$$

$$Order\ 2: \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} since \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$$

$$Order\ 2: \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} since \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$$

$$Order\ 2: \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} since \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$$

$$Order\ 3: \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} since \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$$

$$Order\ 3: \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} since \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} \quad \diamond$$

Of course we have also illustrated that $exp(S_3) = |S_3|$.

We now prove a sequence of three theorems, Theorems 47, 48, 49. The result we want is a corollary, Corollary 50, to the third theorem, Theorem 49, namely the multiplicative group F^* of a finite field F is cyclic.

Theorem 47. *****
Let G be an abelian group with identity e and let $a, b \in G$.
Suppose[3] that $|a| = n$ and $|b| = m$ and $gcd(n,m) = 1$.
Then $|ab| = nm$.
That is, $a^n = e$ and $b^m = e \Rightarrow (ab)^{nm} = e$.

Proof. Let G be an abelian group with identity e and let $a, b \in G$. Let $|a| = n$ and $|b| = m$ and $gcd(n,m) = 1$.

[2]The least common multiple of a set of integers is the smallest integer they all divide into.
[3]Recall Definition 13, page 33, the order of a group element.

Because G is abelian,

$$(ab)^{nm} = abab\cdots ab = aa\cdots abb\cdots b = a^{nm}b^{nm} = (a^n)^m(b^m)^n = e^m e^n = e.$$

Now if the order of ab is t, that is $(ab)^t = e$, then $(ab)^{nm} = e$ can only be true if $t|nm$, that is, $nm = kt, k \in \mathbb{N}$, so that we can have,

$$(ab)^{nm} = (ab)^{kt} = ((ab)^t)^k = e^k = e.$$

Thus, the order t of ab divides nm. Now,

$$(ab)^t = e \Rightarrow a^t b^t = e \Rightarrow a^t = b^{-t} \Rightarrow a^{tm} = b^{-tm}$$

But,

$$b^{-tm} = (b^m)^{-t} = e^{-t} = e \Rightarrow a^{tm} = e$$

Now by Corollary 60A on page 111, since $gcd(n, m) = 1$ we may write $1 = rn + sm$ for some $r, s \in \mathbb{Z}$. Then, multiplying both sides by n,

$$t = trn + tsm.$$

Therefore, as $a^{tm} = e$, we see that since,

$$a^{stm} = (a^{tm})^s = e^s = e \text{ and } a^{trn} = (a^n)^{tr} = e^{tr} = e,$$

then,

$$a^t = a^{tms+trn} = a^{tms}a^{trn} = e \cdot e = e.$$

Again, as argued above for $t = |ab|$ if $|a| = n \Leftrightarrow a^n = e$, we can only have $a^t = e$ if $t = nk, k \in \mathbb{N}$, so that,

$$a^t = a^{nk} = (a^n)^k = e^k = e.$$

This means $n|t$.
Similarly, $m|t$.
Thus, $nm|t$ because $gcd(n, m) = 1$.
We have therefore proved that nm divides t.
But we showed above that t divides nm.
Therefore, $t = nm$ so that $|ab| = nm = |a| \cdot |b|$. □

We prove in the following theorem that in an abelian group G there is an element with order $exp(G)$.

Theorem 48. *****
Let G be an abelian group with identity e and let $a, b \in G$.
Suppose that $|a| = n$ and $|b| = m$ and $lcm(n, m) = k$.
Then there is an element $c \in G$ with order $|c| = k$.
That is there is an element in G with order $exp(G)$.

Proof. By the Fundamental Theorem of Arithmetic, Theorem 65A, page 117, we may write any number as a product of primes and specifically,

$$n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r} \text{ and } m = p_1^{f_1} p_2^{f_2} \dots p_r^{f_r}$$

for some distinct primes $p, p_2, \dots p_r$ and integers $e_i, f_i \geq 0$.
If $s_i = max(e_i, f_i)$ and $k = lcm(n, m)$, then by definition of the least common multiple[4], if $k = lcm(n, m)$ then, $k = p_1^{s_1} p_2^{s_2} \dots p_r^{s_r}$.
For each i put $n_i = \dfrac{n}{p_i^{e_i}} \Leftrightarrow n = n_i p_i^{e_i}$.
Now $|a| = n \Rightarrow (a^{n_i})^{p_i^{e_i}} = a^{\frac{n}{p_i^{e_i}} \cdot p_i^{e_i}} = a^n = e$ so that $|a^{n_i}| = p_i^{e_i}$. Similarly, we can prove $|b^{m_i}| = p_i^{f_i}$.
From $(a^{n_i})^{p_i^{e_i}} = e$ and $(b^{m_i})^{p_i^{f_i}} = e$ we identity $s_i = max(e_i, f_i)$. We may assume $f_i \geq e_i$. If not we can simply interchange e_i, f_i in the proof that follows.
Then, with $s_i = f_i$,

$$(a^{n_i} b^{m_i})^{p_i^{s_i}} = (a^{n_i})^{p_i^{f_i}} (b^{m_i})^{p_i^{f_i}} = (a^{n_i})^{p_i^{f_i}} \times e = (a^{n_i})^{p_i^{e_i} \cdot p^{f_i - e_i}} = e^{p^{f_i - e_i}} = e$$

Accordingly, with $s_i = max(e_i, f_i)$, for each i we may find an element $c_i = a^{n_i} b^{m_i}$ of order $p_i^{s_i}$.
Set $c = c_1 c_2 \dots c_r$. Then using induction, to show $|c_1 c_2 \cdots c_r| = |c_1||c_2| \cdots |c_r|$ we argue,
Basis Step: If $r = 2, |c_1 c_2| = |c_1||c_2|$ by Theorem 47 above.
Induction Step: Suppose $|c_1 c_2 \cdots c_{r-1}| = |c_1||c_2| \cdots |c_{r-1}|$
Then,

$$\begin{aligned} |c_1 c_2 \cdots c_r| &= |c_1 c_2 \cdots c_{r-1}||c_r| \textit{ by basis step} \\ &= |c_1||c_2| \cdots |c_r| \textit{ by the supposition.} \end{aligned}$$

so,

$$|c| = |c_1 c_2 \dots c_r| = |c_1||c_2| \dots |c_r| = p_1^{s_1} p_2^{s_2} \dots p_r^{s_r} = k,$$

or the order of $c = c_1 c_2 \cdots c_r$ is $k = exp(G)$.
So there is an element of G with order $exp(G)$. □

Theorem 49. *****
Let G be a finite abelian group. Then G is cyclic if and only if $exp(G) = |G|$.

[4]For example, suppose $n = 12 = 2^2 3^1 5^0$, $m = 20 = 2^2 3^0 5^1$, then $k = lcm(n, m) = 2^2 3^1 5^1 = 60$ where the exponents of k are the respective maxima of the powers of primes in the expansions of n, m.

Proof. Suppose G is cyclic. By Lagrange's Theorem 23 on page 64, each element of a finite group G has order dividing $|G|$.
Thus, the *lcm* of the orders of all the elements divides $|G|$ or $exp(G)$ divides $|G|$.
Now if $G =< g >$ is a cyclic group of order n, that is, $|G| = n$, then g has order n or $|g| = n$ by Theorem 4, page 33.
We claim that in a cyclic group, the order of every other element in the group also divides n making $exp(G) = n = |G|$.

The proof of the claim is as follows.
If $g^k = e$ and $k \nmid n$ then write $k = xn + y,\ 0 \leq y < n$ by the Division Algorithm 57A, page 105.
Then $g^k = g^{xn+y} = (g^n)^x g^y = g^y = e$ and since $y < n$ this is a contradiction to the minimality of n as the smallest integer for which $g^n = e$, so $k|n$.
So, the order of every other element in the group also divides n making
$exp(G) = n = |G|$.

*****

Conversely, suppose that $exp(G) = |G|$. By the previous Theorem 48, there is an element $g \in G$ of order $exp(G)$, that is, $|g| = exp(G)$.
Thus, since $exp(G) = |G|$, making $|g| = |G|$, we see by Theorem 4(3)[5] that
$G =< g >$, so G is cyclic. □

Finally we prove the corollary that the multiplicative group of a finite field is cyclic.

Corollary 50. *****
Let F be a finite field with multiplicative group $F^\times$. Then $F^\times$ is cyclic.

Proof. Since $F^\times$ is finite and abelian, the conditions of the previous Theorem 49 apply, so it is enough to prove that $exp(F^\times) = |F^\times|$.
Let $exp(F^\times) = m$ and $|F^\times| = n$. Then each element of $F^\times$ has order dividing m, by definition of the exponent.
Thus, $g^m = 1$ for each $g \in F^\times$. Therefore, each element of $F^\times$ is a root of $x^m - 1$.
This makes $|F^\times| \leq deg(x^m - 1) = m$, so $n \leq m$.
But, by Lagrange's Theorem 23[6], the order of every element of $F^\times$ divides $|F^\times|$. Then the $exp(F^\times)$ or the *lcm* of all the elements of $F^\times$ divides $F^\times$.
Hence m divides n or $m \leq n$. But earlier we saw $n \leq m$, thus, $m = n$ or
$exp(F^\times) = |F^\times|$.
By Theorem 49, $F^\times$ is cyclic. □

[5]Theorem 4(3) on page 33 states a finite group G is cyclic if and only if there exists an element $a \in G$ such that the order of a equals the order of G, that is, $|a| = |G|$.

[6]Lagrange's Theorem on page 64 proves that if $a \in G$ then $|a|$ divides $|G|$.

Chapter 8

The Rings of Integers and Polynomials

8.1 Working with Polynomials

Recall, a polynomial has the form,

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

We will refer to the coefficients as $a_i, 0 \leq i \leq n$ or simply as the a_i.

Notation 4. *Given a field F, the complete set of polynomials in the variable x with $a_i \in F$ is denoted by $F[x]$.*

We will now explore $F[x]$. The results we obtain parallel the results you already know from your high school and college algebra courses for polynomials whose coefficients are integers, polynomials such as $x^3 + 3x^2 - 2x + 1$. Again, it is a question of abstraction. The polynomials you are familiar with are $f(x) \in \mathbb{Z}[x]$, meaning their coefficients are integers. We are broadening to polynomials whose coefficients are in ANY field. For instance, if $f(x) \in \mathbb{Q}(\sqrt{2})[x]$, then we might be dealing with not $x^3 + 3x^2 - 2x + 1$ but $x^3 + 3\sqrt{2}x^2 - (2 - 5\sqrt{2})x + 17 - 6\sqrt{2}$.

Definition 46. *addition and multiplication of polynomials*
The addition of two polynomials,

$$f(x) = a_m x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0$$
$$g(x) = b_n x^n + b_{n-1}x^{n-1} + \ldots + b_1 x + b_0$$

is defined by just adding the coefficients of the terms with the same power of x. Assuming[1] *$m \geq n$ we can extend $g(x)$ and write,*

$$g(x) = b_m x^m + \ldots + b_{n+1}x^{n+1} + b_n x^n + b_{n-1}x^{n-1} + \ldots + b_1 x + b_0$$

[1] If $m < n$ then extend $f(x)$ rather than $g(x)$ in similar fashion.

where $b_j = 0$ *for* $n < j \leq m$, *and then,*

$$f(x) + g(x) = \sum_{i=0}^{m} (a_i + b_i)x^i.$$

Their product is defined to be,

$$\begin{aligned} f(x) \cdot g(x) &= (a_m x^n + a_{m-1}x^{n-1} + \ldots + a_1 x + a_0)(b_n x^n + b_{n-1}x^{n-1} + \ldots + b_1 x + b_0) \\ &= a_m b_n x^{m+n} + \ldots + (a_2 b_0 + a_1 b_1 + a_0 b_2)x^2 + (a_1 b_0 + a_0 b_1)x + a_0 b_0 \\ &= \sum_{k=0}^{m+n} c_k x^k, \quad c_k = \sum_{i=0}^{k} a_i b_{k-i} = \sum_{i+j=k} a_i b_j \end{aligned}$$

Using these definitions we prove in Theorem 51 that $F[x]$ is a commutative ring with identity and we then prove a theorem, plus a corollary proving cancellation, that morphs into factors.

Theorem 51. ****
$F[x]$ is a commutative ring with identity, (it has parallel properties to the integers), that is the following properties hold for all $f(x), g(x), h(x) \in F[x]$.

Associative laws:

$$\begin{aligned} f(x) + (g(x) + h(x)) &= (f(x) + g(x)) + h(x) \\ f(x) \cdot (g(x) \cdot h(x)) &= (f(x) \cdot g(x)) \cdot h(x) \end{aligned}$$

Commutative laws:

$$\begin{aligned} f(x) + g(x) &= g(x) + f(x) \\ f(x) \cdot g(x) &= g(x) \cdot f(x) \end{aligned}$$

Distributive laws:

$$\begin{aligned} f(x) \cdot (g(x) + h(x)) &= f(x) \cdot g(x) + f(x) \cdot h(x) \\ (f(x) + g(x))h(x) &= f(x) \cdot h(x) + g(x) \cdot h(x) \end{aligned}$$

Identity elements:
$f(x) = 0$ and $f(x) = 1$ serve as the additive and multiplication identity elements respectively of $F[x]$.

Additive inverses:
Since each coefficient $a_i \in F$ has an inverse $a_i^{-1} \in F$, the polynomial $-f(x)$ is the additive inverse of $f(x)$.

Proof. Except for the distributive law[2] the proofs are very easy through writing out each side of the respective equality in terms of the definitions preceding the statement of the theorem just as we do in the next proof. □

Theorem 52. ** *If $f(x), g(x)$ are nonzero polynomials in $F[x]$, then,*

$$deg(f(x)g(x)) = deg(f(x)) + deg(g(x)).$$

Proof. Let,

$$f(x) = a_m x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0$$
$$g(x) = b_n x^n + b_{n-1}x^{n-1} + \ldots + b_1 x + b_0,$$

where $deg(f(x)) = m,\ deg(g(x)) = n$. Thus $a_m \neq 0,\ b_n \neq 0$.
Since, by Definition 46, page 100, the leading coefficient in $f(x)g(x)$ is $a_m b_n$, the leading term in x is x^{m+n} which has degree $m + n = deg(f(x)) + deg(g(x))$. □

---

[2]To prove the distributive law, consider the polynomials $\sum_{i=0}^{m} a_i x^i, \sum_{j=0}^{n} b_j x^j, \sum_{k=0}^{p} c_k x^k$. We have, assuming without loss of generality that $n > p$,

$$\sum_{i=0}^{m} a_i x^i \left(\sum_{j=0}^{n} b_j x^j + \sum_{k=0}^{p} c_k x^k \right) = \sum_{i=0}^{m} a_i x^i \left(b_n x^n + \ldots + b_0 + c_p x^p + \ldots c_0 \right)$$
$$= \sum_{i=0}^{m} a_i x^i \sum_{l=0}^{n} (b_l + c_l) x^l \text{ where } c_l = 0 \text{ for } n > p$$

Now the first sum and the second sum are independent of one another so we can take the first sum inside the second sum thus,

$$= \sum_{l=0}^{n} \left(\sum_{i=0}^{m} a_i x^i \right) (b_l + c_l) x^l \text{ where } c_l = 0 \text{ for } l > p$$

and use the distributive law of the reals thus,

$$= \sum_{l=0}^{n} \left(\sum_{i=0}^{m} a_i x^i \right) b_l x^l + \sum_{l=0}^{n} \left(\sum_{i=0}^{m} a_i x^i \right) c_l x^l$$

and then again using the independence of the $a_i x^i$ sum, we obtain the desired result,

$$= \left(\sum_{i=0}^{m} a_i x^i \right) \sum_{l=0}^{n} b_l x^l + \left(\sum_{i=0}^{m} a_i x^i \right) \sum_{l=0}^{n} c_l x^l$$
$$= \left(\sum_{i=0}^{m} a_i x^i \right) \sum_{l=0}^{n} b_l x^l + \left(\sum_{i=0}^{m} a_i x^i \right) \sum_{l=0}^{p} c_l x^l \text{ since } c_l = 0 \text{ for } l > p.$$

Note 17. *Let's look at polynomial cancellation of common factors. We prove if* $f(x), g(x), h(x) \in F[x]$ *and* $f(x)$ *is not the zero polynomial, then,*

$$f(x)g(x) = f(x)h(x) \Rightarrow g(x) = h(x).$$

The proof is as follows.

$$\begin{aligned} & f(x)g(x) = f(x)h(x) \\ \Rightarrow\ & f(x)g(x) - f(x)h(x) = 0 \\ \Rightarrow\ & f(x)[g(x) - h(x)] = 0 \quad \textit{distributive law} \\ \Rightarrow\ & g(x) - h(x) = 0 \quad \textit{since } f(x) \neq 0 \\ \Rightarrow\ & g(x) = h(x) \end{aligned}$$

Definition 47. *factor or divisor*
We say $g(x) \in F[x]$ *is a factor or divisor of* $f(x) \in F[x]$ *if there is a* $p(x) \in F[x]$ *such that* $f(x) = g(x)p(x)$*, and we write* $g(x) \mid f(x)$*.*

Notation 5. *The set of all polynomials in* $F[x]$ *that are divisible by* $g(x)$ *is denoted by* $< g(x) >$ *. In other words* $f(x) \in < g(x) >$ *if* $f(x) = g(x)p(x)$ *for some polynomial* $p(x) \in F[x]$*.*
Further, under addition, $< g(x) >$ *is a subgroup of* $F[x]$ *since, by the subgroup test, if* $p(x), q(x) \in < g(x) >$ *then, given the inverse of* $p(x)$ *is simply* $-p(x)$*, under the group operation of addition of polynomials, we have* $q(x) - p(x) \in < g(x) >$ *. Accordingly, by Corollary 3, page 31,* $< g(x) >$ *is a subgroup of* $F[x]$*.*

In the final section of Chapter 8 we will prove a key theorem dealing with a factor group $F[x]/ < p(x) >$. We prove it is a field.

Example 42.

$$\begin{aligned} f(x) &= x^5 + x^3 + 3x^2 + 3 \\ &= (x^2 + 1)(x^3 + 3) \end{aligned}$$

makes $f(x) \in < x^2 + 1 >$ *and* $f(x) \in < x^3 + 3 >$ *.* $\diamond$

We next prove, via Theorems 53 and 54, the Factor Theorem 55, that c is a root or solution of the polynomial equation $f(x) = 0$ if and only if $f(c) = 0$, that is, $x - c \mid f(x)$.

Theorem 53. ***
For any element $c \in F$ *and any positive integer* k*,*

$$(x - c) \mid (x^k - c^k).$$

Proof. If we multiply out $(x - c)(x^{k-1} + cx^{k-2} + \ldots + c^{k-2}x + c^{k-1})$ we get $x^k - c^k$. $\square$

Theorem 54. ** (Remainder Theorem)*
Let $f(x) \in F[x]$ be a nonzero polynomial and let $c \in F$. Then there exists a polynomial $q(x) \in F[x]$ such that,

$$f(x) = q(x)(x-c) + f(c)$$

That is, when $f(x)$ is divided by $x-c$ the remainder is $f(c)$.

Proof. Let $f(x) \in F[x]$ be,

$$f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0,\ a_i \in F$$

Since by Theorem 53 every term in,

$$f(x) - f(c) = a_m(x^m - c^m) + a_{m-1}(x^{m-1} - c^{m-1}) + \cdots + a_1(x-c)$$

is divisible by $(x-c)$, then for some $q(x) \in F[x]$, we can write,

$$\begin{aligned} f(x) - f(c) &= (x-c)q(x) \\ \Rightarrow f(x) &= (x-c)q(x) + f(c). \end{aligned}$$

So when $f(x)$ is divided by $(x-c)$ the remainder is $f(c)$. □

Corollary 55. ** (Factor Theorem)*
Let $f(x) \in F[x]$ be a nonzero polynomial and let $c \in F$. Then c is a root or zero of $f(x)$ if and only if $(x-c)$ is a factor of $f(x)$.
That is $f(c) = 0$ if and only if $(x-c) \mid f(x)$ or $f(x) = (x-c)g(x)$, where $g(x)$ is a polynomial of one less degree than $f(x)$.

Proof. From Theorem 54 we have $f(x) = (x-c)q(x) + f(c)$.
Clearly, if $f(c) = 0$ then $f(x) = (x-c)q(x)$, that is $(x-c)$ is a factor of $f(x)$.

*****

Conversely, if $f(x) = (x-c)q(x)$ then $f(c) = (c-c)q(c) = 0$. □

The Factor Theorem is an invaluable tool in factoring polynomials.

Example 43. *For example, if $f(x) = x^3 - x^2 - x + 1$ has factors such as,*

$$f(x) = (x-r_1)(x-r_2)(x-r_3),$$

the r_i can only be ± 1. So we calculate,

$$\begin{aligned} f(1) &= 1 - 1 - 1 + 1 = 0 \\ f(-1) &= -1 - 1 - 1 - 1 \neq 0 \end{aligned}$$

and conclude $(x-1)$ is a factor but $(x+1)$ is not. By long (or synthetic) division we find the other factor is x^2+1, giving $f(x) = (x-1)(x^2+1)$. ◇

We finish this section with Corollary 56 that a polynomial of degree n with coefficients in F has at most n distinct roots in F.

Corollary 56. ***
A polynomial $f(x) \in F[x]$ of degree n with coefficients in the field F has at most n distinct roots in F. Equivalently, $f(x)$ can have at most n distinct factors.

Proof. Let $f(x) \in F[x]$ have degree n.
If $(x-c)$ is a factor of $f(x)$ then we can write $f(x) = (x-c)g(x)$ where $g(x)$ has degree 1 less than $f(x)$. We can repeat this process, saying if $(x-b)$ is a factor of $g(x)$ then we can write $f(x) = (x-c)(x-b)h(x)$ where $h(x)$ has degree 2 less than $f(x)$. But we cannot repeat this process more than n times. □

We next establish a series of definitions and proofs for polynomials that parallel the series of definitions and proofs for the integers. We label the parallel definitions and theorems as A and B.

The comparability is not surprising in the sense that they are both commutative rings with identity but it is surprising in the sense that a polynomial and an integer are totally different objects. This is a beautiful example of mathematical abstraction, in this case, of rings.

The result we need is the final theorem in this chapter.

8.2 Division algorithm

8.2.1 Division Algorithm for Integers

It is simple for us to agree if we divide, say 46 by 7, then the remainder 4 is less than 7, but let's formalize this.

Theorem 57A. ** (Division Algorithm for Integers)*
For every $a, b \in \mathbb{Z}$ there exist a unique pair $q, r \in \mathbb{Z}$ such that,

$$a = bq + r,\ 0 \le r < b.$$

Proof. For this proof we need to accept the Well-Ordering principle which states that every non-empty set of the positive integers contains a smallest element.
Let S be the set of positive integers that are greater than a/b. By the Well-Ordering principle S contains a smallest element t, that is, we can construct the inequality,

$$t - 1 \le \frac{a}{b} < t.$$

Let $q = t - 1 \Leftrightarrow t = q + 1$, multiply through by b and subtract qb from all the terms. Then,

$$qb \le a < (q+1)b \Rightarrow 0 \le a - qb < b$$

Putting $r = a - qb$ gives us the desired result $a = qb + r$.
Then, substituting this result into $0 \le a - qb < b$ we also obtain $0 \le r < b$. □

Example 44. $67, 12 \in \mathbb{Z}$ *and* $67 = 12 \cdot 5 + 7$ *where* $7 < 12$.

8.2.2 Division Algorithm for Polynomials

Similarly, if we divide a polynomial such as x^5+1 by x^2+1 then the remainder $(-x+1)$ will have degree one less than the degree of x^2+1 but let's formalize this.

Theorem 57B. *** (Division Algorithm for polynomials)*
If F is a field, for any polynomials $f(x), g(x) \in F[x]$ where $g(x) \neq 0$, there exist unique polynomials $q(x), r(x)$ such that,

$$f(x) = q(x)g(x) + r(x)$$

where either $deg(r(x)) < deg(g(x))$ or $r(x) = 0$.

Proof. Let,

$$f(x) = a_m x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0 \in F[x], \tag{8.2.1}$$
$$g(x) = b_n x^n + b_{n-1}x^{n-1} + \ldots + b_1 x + b_0 \in F[x], \tag{8.2.2}$$

and consider the set

$$S = \{f(x) - g(x)s(x) \mid s(x) \in F[x]\}$$

Of all the elements $f(x) - g(x)s(x)$, choose $s(x) = q(x)$ to make $f(x) - g(x)q(x)$ any one of the elements of S with least degree.[3] Set,

$$r(x) = f(x) - g(x)q(x)$$

so that $r(x)$ has minimal degree in S. Then,

$$f(x) = g(x)q(x) + r(x)$$

We must show $deg(r(x)) < n = deg(g(x))$. Suppose,

$$r(x) = c_t x^t + c_{t-1}x^{t-1} + \cdots + c_1 x + c_0, \tag{8.2.3}$$

[3]For example if $F = \mathbb{Q}$, suppose,

$$f(x) = 3x^4 + x^3 - 1$$
$$g(x) = 2x^2 + x + 1$$

Then we can choose $s(x) = \frac{3}{2}x^2 - \frac{1}{4}x - \frac{5}{8}$ so that,

$$f(x) - g(x)s(x) = \frac{7}{8}x - \frac{3}{8}$$

which has degree 1 and this is the least degree of all the polynomials in $\{f(x) - g(x)s(x)\}$ since it is not possible to choose the coefficients of the general $s(x) = ax^2 + bx + c$ to have $f(x) - g(x)s(x)$ equal to a polynomial of zero degree (a constant). Note $r(x) = \frac{7}{8}x - \frac{3}{8}$ has degree less than the degree of $g(x) = 2x^2 + x + 1$.

where the coefficients c_i are elements in F and $c^t \neq 0$ if $t \neq 0$. We suppose $t \geq n$, and prove this is a false supposition, hence $t < n$.
Subtracting $\frac{c_t}{b_n}x^{t-n}g(x)$ from both sides, we have from $f(x) - g(x)q(x) = r(x)$, that,

$$f(x) - g(x)q(x) - \frac{c_t}{b_n}x^{t-n}g(x) = r(x) - \frac{c_t}{b_n}x^{t-n}g(x) \tag{8.2.4}$$

But the right side of (8.2.4) is,

$$\begin{aligned} & r(x) - \frac{c_t}{b_n}x^{t-n}(b_n x^n + b_{n-1}x^{n-1} + \ldots + b_1 x + b_0) \\ &= r(x) - c_t x^t + \cdots \\ &= (c_t x^t + c_{t-1}x^{t-1} + \cdots + c_1 x + c_0) - c_t x^t + \cdots \qquad \text{by (8.2.3)} \\ &= \cancel{c_t x^t} + c_{t-1}x^{t-1} + \cdots + c_1 x + c_0 - \cancel{c_t x^t} + \cdots \end{aligned}$$

which is a polynomial of degree less than the degree of $r(x)$ which is t.
However, the left side of (8.2.4), which must also have degree less than t can be written as

$$f(x) - g(x)q(x) - \frac{c_t}{b_n}x^{t-n}g(x) = f(x) - g(x)\left(q(x) - \frac{c_t}{b_n}x^{t-n}\right)$$

so it is in the set $S = \{f(x) - g(x)s(x) \mid s(x) \in F[x]\}$ with, since it equals the right side, degree less than that of $r(x)$ contradicting the fact that $r(x)$ has minimal degree in S.
So the supposition $t \geq n$ is false. Therefore the degree of $r(x)$ is less than $n = deg(g(x))$.

*****

We can show $q(x), r(x)$ are unique by supposing,

$$f(x) = g(x)q_1(x) + r_1(x),\ deg(r_1(x)) < deg(g(x)) \tag{8.2.5}$$
$$f(x) = g(x)q_2(x) + r_2(x),\ deg(r_2(x)) < deg(g(x) \tag{8.2.6}$$

We note

$$deg(r_2(x) - r_1(x)) < deg(g(x)) \tag{8.2.7}$$

Subtracting the two equations (8.2.5) and (8.2.6) for $f(x)$, we find,

$$g(x)[q_1(x) - q_2(x)] = [r_2(x) - r_1(x)]$$

Now the factors of a polynomial obviously have degree less than that of the polynomial.
Here, if $q_2(x) - q_1(x) \neq 0$ then $deg(r_2(x) - r_1(x)) \geq deg(g(x))$.
This contradiction to (8.2.7) must mean $q_2(x) - q_1(x) = 0$ giving $q_2(x) = q_1(x)$.
In turn this means $r_2(x) - r_1(x) = 0$ so that $r_2(x) = r_1(x)$.
This proves uniqueness. □

Example 45. *For example, with* $f(x) = x^3 + 2x + 2$ *and* $g(x) = x^2 + x + 1$, *we have,*

$$x^3 + 2x + 2 = (x^2 + x + 1)(x - 1) + (2x + 3)$$

where $deg(2x + 3) = 1$ *is less than* $deg(x^2 + x + 1) = 2$. ◇

8.3 Greatest Common Divisor

8.3.1 Integers

Definition 48A. *greatest common divisor for integers*
The greatest common divisor of the integers $a, b \in \mathbb{Z}$ *is denoted by* $gcd(a, b)$ *and is the largest integer* $d \in \mathbb{Z}$ *that divides both* a *and* b.
If $gcd(a, b) = 1$ *we say* a *and* b *are relatively prime.*

Example 46.

$$gcd(27, 18) = 9$$
$$gcd(23, 17) = 1 \qquad \diamond$$

Theorem 59A. ***
(a) Let a *and* b *be integers and* $d = gcd(a, b)$. *Then* d *is the smallest positive integer that can be expressed as a linear combination* $ax + by$ *of* a *and* b, *that is,* $d = ax + by$.
(b) There exist integers x, y *satisfying* $ax + by = c$ *iff* $d|c$ *where* $d = gcd(a, b)$.

Proof. We prove the two statements separately.
(a) Let a and b be integers and $d = gcd(a, b)$. By the Well Ordering principle[4], the set of all linear combinations of a and b contains a smallest positive element m, say $m = sa + tb$.
We want to prove $m = gcd(a, b) = d$.
By the Division Algorithm, Theorem 57A on page 105, we can write,

$$a = qm + r, \ 0 \le r < m. \tag{8.3.1}$$

Then, using $m = sa + tb$,

$$r = a - qm = a - q(sa + tb) = (1 - qs)a + (-tq)b,$$

so r is a linear combination of a and b.
But by (8.3.1) $0 \le r < m$ and m is the smallest positive element of the set of all possible linear combinations of a and b. This contradiction gives us $r = 0$ and $a = qm$ or $m|a$.
By a similar argument applied to $b = qm + r, \ 0 \le r < m$ we obtain $m|b$.

[4]Recall, the Well Ordering Principle is an axiom of the natural numbers. It states that every non-empty set of natural numbers contains a smallest element.

Then m is a common divisor of a and b.
Now since $d|a$ and $d|b$ then[5] $d|(sa+tb)$ so that $d|m$ making $d \le m$.
Since d is the greatest common divisor, we cannot have $d < m$ so we must have $d = m$ which proves (a), namely $d = gcd(a,b)$ is the smallest positive integer that can be expressed as a linear combination $ax + by$.

****

(b) We want to prove there exist integers x, y satisfying $ax + by = c$ iff $d|c$ where $d = gcd(a,b)$.
First assume $ax + by = c$ holds. We want to prove $d|c$.
For $d = gcd(a,b)$, let $a = ed, b = fd$. Then,

$$c = ax + by = edx + fdy = d(ex + fy) \Rightarrow d|c.$$

*****

Conversely, assume $d|c$, say $kd = c$. We want to prove there exist integers x, y satisfying $ax + by = c$.
Now by Part (a), there exist x', y' such that $ax' + by' = d$. Hence, multiplying by k,

$$a(x'k) + b(y'k) = dk = c$$

In other words, $x = x'k$ and $y = y'k$ are a solution of $ax + by = c$.
This proves Part (b). □

8.3.2 Polynomials

Definition 48B. *greatest common divisor for polynomials*
If F is a field, the greatest common divisor of the polynomials $f(x), g(x) \in F[x]$ is denoted by $gcd(f(x), g(x))$ and is the polynomial $d(x) \in F[x]$ of largest degree that divides both $f(x)$ and $g(x)$.
If $gcd(f(x), g(x)) = 1$ we say $f(x)$ and $g(x)$ are relatively prime.

Example 47.

$$gcd(x^3 + 1, x^5 + 1) = x + 1,$$
$$gcd(x^3 + 1, x^2 + 1) = 1.$$

We now consider the parallel gcd theorem for polynomials.

Theorem 58B. ***
Where F is a field, for any nonzero polynomials $f(x), g(x) \in F[x]$, the greatest common divisor $d(x) = gcd(f(x), g(x))$ exists and can be expressed as a linear combination of $f(x)$ and $g(x)$ in the form,

$$d(x) = a(x)f(x) + b(x)g(x)$$

for some $a(x), b(x) \in F[x]$.

[5] If $a = dx, b = dy$ then $sa + tb = sdx + tdy = d(sx + ty) \Rightarrow d|(sa + tb)$.

Proof. Let $f(x), g(x) \in F[x]$. Consider the set of polynomials,

$$G[x] = \{a(x)f(x) + b(x)g(x) \mid a(x), b(x) \in F[x]\}$$

Let $d(x)$ be an element of $G[x]$ of minimal, or smallest possible, degree. Then,

$$d(x) = a(x)f(x) + b(x)g(x) \tag{8.3.2}$$

for some $a(x), b(x) \in F[x]$. By the Division Algorithm 57B, page 106, we have,

$$f(x) = q(x)d(x) + r(x),\ deg(r(x)) < deg(d(x))\ or\ r(x) = 0$$

Then,

$$r(x) = f(x) - q(x)d(x)$$

But this means $r(x) \in G[x]$ and has degree less than that of $d(x)$. This is a contradiction unless $r(x) = 0$.
But then $f(x) = q(x)d(x)$ which means $d(x) \mid f(x)$.
By a similar argument we have $d(x) \mid g(x)$ and hence $d(x)$ is a common divisor of $f(x)$ and $g(x)$.

*****

To show $d(x)$ is the greatest common divisor of $f(x), g(x)$ we need to show any other divisor of both $f(x)$ and $g(x)$ divides $d(x)$.
So, suppose some other $h(x) \in G[x]$ divides both $f(x)$ and $g(x)$, say,

$$f(x) = h(x)j(x) \text{ and } g(x) = h(x)k(x) \tag{8.3.3}$$

Then since $d(x) \in G[x]$, by (8.3.2),

$$d(x) = a(x)f(x) + b(x)g(x)$$

for some $a(x), b(x) \in F[x]$. Thus we have, substituting from (8.3.3),

$$\begin{aligned} d(x) &= a(x)h(x)j(x) + b(x)h(x)k(x) \\ &= h(x)[a(x)j(x) + b(x)k(x)] \\ &\Rightarrow h(x) \mid d(x), \end{aligned}$$

which means any other common divisor $h(x)$ has degree less than the degree of $d(x)$. Thus $d(x)$ is the greatest common divisor of $f(x), g(x)$. □

We can also prove Theorem 59B by quoting the procedure used in proving the Euclidean Algorithm 61B in the next section.

Theorem 59B. *** (Alternative proof)*
Where F is a field, for any nonzero polynomials $f(x), g(x) \in F[x]$, the greatest common divisor $gcd(f(x), g(x))$ exists and can be expressed as a linear combination of $f(x)$ and $g(x)$ in the form,

$$gcd(f(x), g(x)) = a(x)f(x) + b(x)g(x)$$

for some $a(x), b(x) \in F[x]$.

Proof. In the proof of the Euclidean Algorithm, Theorem 61B, for polynomials on page 114 we have the sequence of equations,

$$\begin{aligned}
r_{n-2}(x) &= q_n(x)r_{n-1}(x) + r_n(x) \\
r_{n-3}(x) &= q_{n-1}(x)r_{n-2}(x) + r_{n-1}(x) \\
r_{n-4}(x) &= q_{n-2}(x)r_{n-3}(x) + r_{n-2}(x) \\
&\dots \\
g(x) &= q_2(x)r_1(x) + r_2(x) \\
f(x) &= q_1(x)g(x) + r_1(x)
\end{aligned}$$

From this sequence we have that $r_n(x)$ is a common divisor of $f(x)$ and $g(x)$ and we can then "backtrack" to form the sequence of equations,

$$\begin{aligned}
r_n(x) &= r_{n-2}(x) - q_n(x)r_{n-1}(x) \\
&= r_{n-2}(x) - q_n(x)[r_{n-3}(x) - q_{n-1}(x)r_{n-2}(x)] \\
&\dots \\
&= r_{n-4}(x)[1 + q_n(x)q_{n-1}(x)] - r_{n-3}(x)[q_{n-2}(x) + q_n(x)q_{n-1}(x)q_{n-2}(x) + q_n(x)] \dots \\
&= a(x)f(x) + b(x)g(x)
\end{aligned}$$

where $a(x)$ and $b(x)$ are a combination of the $q_i(x)$. So now we have the proof that a common divisor $r_n(x)$ of $f(x)$ and $g(x)$ exists and can be expressed as a linear combination of $f(x)$ and $g(x)$ in the form,

$$r_n(x) = a(x)f(x) + b(x)g(x)$$

for some $a(x), b(x) \in F[x]$. We can then prove $r_n(x)$ is the greatest common divisor as in the previous theorem. □

The Corollaries

Corollary 60A. ***
There exist integers x, y satisfying $ax + by = 1$ iff $gcd(x, y) = 1$.

Example 48. *For example, given $gcd(7, 11) = 1$, we can construct*

$$7 \times 8 - 11 \times 5 = 1. \qquad \diamond$$

Corollary 60B. *
If $f(x), g(x)$ are relatively prime, that is $gcd(f(x), g(x)) = 1$, we can find $a(x), b(x) \in F[x]$ such that

$$f(x)a(x) + g(x)b(x) = 1$$

Example 49. *For example, given $gcd(x^3+1, x^4+1) = 1$ we can construct (as we do later),*

$$1 = \left(x^4+1\right)\left(\frac{-x^3}{2} + \frac{x^2}{2} + \frac{x}{2}\right) + \left(x^3+1\right)\left(\frac{x^4}{2} - \frac{x^3}{2} - \frac{x^2}{2} - \frac{x}{2} + 1\right) \qquad \diamond$$

8.4 Euclidean Algorithm

8.4.1 Euclidean Algorithm for Integers

To find x, y for a given a, b with $gcd(a, b) = 1$, such that $ax + by = 1$ we use the Euclidean Algorithm and repetitions of the Division Algorithm 57A, page 105. The following example demonstrates how the Euclidean Algorithm is to be applied. The proof of the Euclidean Algorithm for integers is the same as that for polynomials on page 121, just omit all the x' s.

Example 50. *For $a, b \in \mathbb{Z}$, using the Division Algorithm we set up the chain of equations which continue until a remainder of 0 is reached, say at r_3,*

$$\begin{aligned} a &= b \cdot q_1 + r_1, & r_1 < b \\ b &= r_1 \cdot q_2 + r_2, & r_2 < r_1 \\ r_1 &= r_2 \cdot q_3 + 0 \\ &\Rightarrow gcd(a, b) = r_2, \end{aligned}$$

Then the gcd is the remainder immediately prior to a remainder of 0.
Then we can backtrack to a as follows. (We went down the chain until we reached a (minimum) remainder of 0 and now we go back up the chain to a.) If, say, we found $r_2 = 1$, then,

$$1 = r_2 = b - r_1 \cdot q_2 = b - (a - bq_1)q_2 \tag{8.4.1}$$

$$\Rightarrow -aq_2 + b(1 + q_1 q_2) = 1 \tag{8.4.2}$$

Let's take $a = 67, b = 13$,

$$\begin{aligned} 67 &= 13 \cdot 5 + 2 \\ 13 &= 2 \cdot 6 + 1 \\ 2 &= 1 \cdot 2 + 0 \\ &\Rightarrow gcd(67, 13) = 1 \end{aligned}$$

which is the least non-zero remainder.
Substituting $a = 67, b = 13, q_1 = 5, r_1 = 2, q_2 = 6, r_2 = 1, q_3 = 2 \Rightarrow 1 + q_1 q_2 = 31$ *into* (8.4.2) *we have,*

$$-67 \cdot 6 + 13 \cdot 31 = 1 \qquad \diamond$$

8.4.2 Euclidean Algorithm for Polynomials

To find $a(x), b(x)$ for a given $f(x), g(x)$ with $gcd(f(x), g(x) = 1$ such that $a(x)f(x) + b(x)g(x) = 1$ we use the Euclidean Algorithm 61B and the Division Algorithm 57B. First an example of how to setup the Euclidean Algorithm.

Example 51. *Let's choose* $f(x) = x^4 + 1,\ g(x) = x^3 + 1$. *Using long division we construct,*

$$\begin{aligned}
x^4 + 1 &= (x^3 + 1)(x) + (-x + 1) \\
x^3 + 1 &= (-x + 1)(-x^2 - x) + (x + 1) \\
-x + 1 &= (x + 1)(-1) + 2 \\
x + 1 &= 2\frac{x}{2} + 1 \\
2 &= 1(2) + 0
\end{aligned}$$

to conclude $gcd(x^4 + 1, x^3 + 1) = 1$, *which is the last non-zero remainder.*
With $f(x), g(x)$ *as chosen and* $a_1(x) = x,\ r_1(x) = -x + 1,\ a_2(x) = -x^2 - x,$ $r_2(x) = x + 1,\ a_3(x) = -1,\ r_3(x) = 2,\ a_4(x) = x/2,\ r_4(x) = 1,\ a_5(x) = 2, r_5(x) = 0$ *we can reframe this as,*

$$\begin{aligned}
f(x) &= g(x)a_1(x) + r_1(x),\ deg(r_1(x) < deg(g(x) \\
g(x) &= r_1(x)a_2(x) + r_2(x) \\
r_1(x) &= r_2(x)a_3(x) + r_3(x) \\
r_2(x) &= r_3(x)a_4(x) + r_4(x) \\
r_3(x) &= r_4(x)a_5(x) + r_5(x),\ r_5(x) = 0 \\
&\Rightarrow gcd(f(x), g(x)) = r_4(x), \quad \textit{which is the last non-zero remainder.}
\end{aligned}$$

Then we can backtrack to $f(x)$ *as follows:*

$$\begin{aligned}
r_4(x) &= 1 \\
&= r_2(x) - r_3(x)a_4(x) \\
&= r_2(x) - [r_1(x) - r_2(x)a_3(x)]a_4(x) \\
&= [g(x) - r_1(x)a_2(x)] - \{(r_1(x) - [g(x) - r_1(x)a_2(x)]a_3(x)\}a_4(x) \\
&= g(x)[1 + a_3(x)a_4(x)] - r_1(x)[a_2(x) + a_4(x) + a_2(x)a_3(x)a_4(x)] \\
&= g(x)[1 + a_3(x)a_4(x)] \\
&\qquad - \{f(x) - g(x)a_1(x)\} \times [a_2(x) + a_4(x) + a_2(x)a_3(x)a_4(x)]
\end{aligned}$$

$$= -f(x)[a_2(x) + a_4(x) + a_2(x)a_3(x)a_4(x)]$$
$$+ g(x)\{[1 + a_3(x)a_4(x)] + a_1(x) \times [a_2(x) + a_4(x) + a_2(x)a_3(x)a_4(x)]\}$$

In our example,
$f(x) = x^4 + 1,\ g(x) = x^3 + 1,\ a_1(x) = x,\quad a_2(x) = -x^2 - x,\ a_3(x) = -1,\ a_4(x) = x/2,$
giving,

$$(x^4 + 1)\left(\frac{-x^3 + x^2 + x}{2}\right) + (x^3 + 1)\left(1 + \frac{x^4 - x^3 - x^2 - x}{2}\right) = 1 \quad \diamond$$

Theorem 61B gives us the strict proof of the Euclidean Algorithm for polynomials or for the integers by deleting all the $(x)s$.

Theorem 61B. *** (Euclidean Algorithm for Polynomials)*
Let F be a field and $f(x), g(x) \in F[x]$. If we apply the Division Algorithm Theorem 57B, page 106, repeatedly,

$$f(x) = q_1(x)g(x) + r_1(x) \qquad (1)$$
$$g(x) = q_2(x)r_1(x) + r_2(x) \qquad (2)$$
$$r_1(x) = q_3(x)r_2(x) + r_3(x) \qquad (3) \qquad \ldots$$

we must come to a finite end since the degree of the remainders is becoming smaller and smaller, so we end with,

$$r_{n-3}(x) = q_{n-1}(x)r_{n-2}(x) + r_{n-1}(x) \qquad (n-1)$$
$$r_{n-2}(x) = q_n(x)r_{n-1}(x) + r_n(x) \qquad (n)$$
$$r_{n-1}(x) = q_{n+1}(x)r_n(x) + r_{n+1}(x) \qquad (n+1)$$

and $r_{n+1}(x) = 0$.
Then the last non-zero remainder $r_n(x) = gcd(f(x), g(x))$.

Proof. From equation $(n+1)$, we have

$$r_{n-1}(x) = q_{n+1}(x)r_n(x) + r_{n+1}(x)$$

Since $r_{n+1}(x) = 0$ we see $r_n(x) \mid r_{n-1}(x)$, say, $r_{n-1}(x) = a(x)r_n(x)$. Substituting into equation (n) gives,

$$r_{n-2}(x) = q_n(x)a(x)r_n(x) + r_n(x) = r_n(x)[q_n(x)a(x) + 1]$$

so that $r_n(x) \mid r_{n-2}(x)$, say $r_{n-2}(x) = b(x)r_n(x)$.
But then from equation $(n-1)$ we see $r_n(x) \mid r_{n-3}(x)$ since

$$r_{n-3}(x) = q_{n-1}(x)r_n(x)b(x) + a(x)r_n(x) = r_n(x)[b(x)q_{n-1}(x) - a(x)],$$

and so on all the way back to equations $(1), (2)$ which show $r_n(x) \mid g(x)$ and finally, $r_n(x) \mid f(x)$ so that $r_n(x)$ is a common divisor of $f(x)$ and $g(x)$.

*****

To show it is the greatest common divisor, suppose $h(x)$ is any other common divisor of $f(x)$ and $g(x)$. Then by equation (1) , $h(x) \mid r_1(x)$, by equation (2) $h(x) \mid r_2(x)$ and so on all the way down the chain of equations till we reach $h(x) \mid r_n(x)$ making $r_n(x)$ the greatest common divisor, that is, $gcd(f(x), g(x)) = r_n(x)$. □

8.5 Primes and Irreducibles

8.5.1 Prime integers

Definition 49A. *prime integer*
A positive integer is a prime number if it cannot be factored into two numbers both greater than 1.
We could say a prime is irreducible.

Example 52. *2,3,5,7,11,13,17,19,23 are primes in* $\mathbb{Z}$.
4,6,8,10,12,14,15,16,18 are called composite numbers.

Theorem 62A. ** (Euclid's Lemma for Integers) If p is a prime and $a, b \in \mathbb{Z}$, then if $p|ab$ either $p|a$ or $p|b$.*

Proof. Suppose $p|ab$, p a prime and $a, b \in \mathbb{Z}$.
Now if p is a prime then either $p|a$ (and we are done) or $p \nmid a$ making $gcd(p, a) = 1$.
In this latter case,by Corollary 60A, page 111 if $gcd(p, a) = 1$ then there exist integers r, s such that,

$$rp + sa = 1 \Rightarrow brp + sab = b \text{ where we multiplied through by } b.$$

Then since $p|ab$ means $ab = pk$ for some $k \in \mathbb{Z}$, we have,

$$brp + spk = b \Rightarrow b = p(br + sk) \Rightarrow p|b.$$

□

Example 53. $3|48 = 6 \times 8$ *and* $3|6$

We can go further.

Corollary 63A. ***
In general, if $p|a_1a_2 \dots a_r$ then $p|a_i$ for at least one a_i, $1 \le i \le r$.

Proof. If $p \nmid a_1$, then $p|a_2a_3 \dots a_r$. Then if $p \nmid a_2$ then $p|a_3a_4 \dots a_r$ and so on. Thus if $p \nmid a_i$, $1 \le i \le r-1$ then we must have $p|a_r$. □

8.5.2 Irreducible polynomials

Definition 49B. *irreducible polynomial*
A polynomial is irreducible over a field F if it cannot be factored in F into polynomials of lesser degree greater than 0.

Example 54. *$x+1, x^2+x+1, x^4+1$ are irreducible in $\mathbb{Q}[x]$.*
$x^3+1=(x+1)(x^2-x+1)$ is reducible in $\mathbb{Q}[x]$. ◇

Theorem 62B. *** (Euclid's Lemma for polynomials)*
With F a field, let $f(x), g(x), p(x) \in F[x]$. If $gcd(p(x), f(x)) = 1$ but $p(x) \mid f(x)g(x)$ then $p(x) \mid g(x)$.

Proof. Suppose $f(x), g(x), p(x) \in F[x]$ and $p(x)|f(x)g(x)$.
Suppose also $gcd(p(x), f(x)) = 1$ so that $p(x) \nmid f(x)$.
By Corollary 60B, page 112, if $gcd(f(x), p(x)) = 1$ then $a(x)f(x) + b(x)p(x) = 1$ for some $a(x), b(x) \in F[x]$.
Multiplying by $g(x)$ gives,

$$g(x) = a(x)g(x)f(x) + b(x)g(x)p(x) \tag{8.5.1}$$

Now,

$$p(x)|f(x)g(x) \Rightarrow f(x)g(x) = h(x)p(x) \text{ for some } h(x) \in F[x].$$

Then, subsituting into (8.5.1),

$$\begin{aligned} g(x) &= a(x)h(x)p(x) + b(x)g(x)p(x) \\ &= p(x)[a(x)h(x) + b(x)g(x)] \\ &\Rightarrow p(x)|g(x) \end{aligned}$$

□

Example 55. *Since $x^3+1=(x+1)(x^2-x+1)$ then $x+1|x^3+1$ requires $x+1$ to divide one of the factors of x^3+1 and indeed, $x+1|x+1$.*

8.6 Unique Factorization

8.6.1 Integers and Unique Factorization

The fundamental theorem of arithmetic is that each integer is able to be factored into the product of primes in a unique way up to order (that is, apart from the order, for example, $12 = 2^2 \times 3 = 3 \times 2^2$).

Theorem 65A. **** (Fundamental Theorem of Arithmetic)*
Every integer $n > 1$ is a product of a unique set of primes. That is,

$$n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_r^{\alpha_r} = \prod_{i=1}^{r} p_i^{\alpha_i}$$

where each p_i is a prime and all $\alpha_i \in \mathbb{N}$.

Proof. To show n is a product of primes, we use a proof by contradiction.
Suppose there is an integer greater than 1 that is not the product of primes.
Then, by the Well-Ordering principle, there must be a smallest one, say m.
Either m is a prime and we are done, or m is not a prime.
In that case, m factors as say, $m = rs$. Since both r and s are smaller than m, they must be the product of primes, and therefore m is also, so we have a contradiction.
We conclude there are no integers greater than 1 that are not a product of primes.

*****

To show n is a product of a unique set of primes, we suppose there are integers greater than 1 with two different factorizations. To find a contradiction, let n be the smallest of these and let two factorizations of n be,

$$n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_r^{\alpha_r} = q_1^{\beta_1} q_2^{\beta_2} q_3^{\beta_3} \dots q_s^{\beta_s} \tag{8.6.1}$$

where the p_i are distinct primes and the q_j are distinct primes and the exponents $\alpha_i, \beta_j \in \mathbb{N}$.
Since p_1 divides the right side, then by Corollary 63A, page 115, p_1 divides $q_j^{\beta_j}$ for some j.
Hence $p_1 = q_j$ since both are prime. Thus we may divide (8.6.1) by p_1 to get two different factorizations of $\dfrac{n}{p_1}$.
But $\dfrac{n}{p_1} < n$, so we have a contradiction since we supposed n is the smallest integer with two different factorizations.
We conclude any integer has a unique factorization into primes. □

Example 56. $720 = 2^4 3^2 5$

8.6.2 Polynomials and Unique Factorization

In order to prove the corresponding theorem for polynomials, we first need Theorem 64B.

Theorem 64B. *****
The non-constant polynomial $p(x) \in F[x]$ is irreducible over $F[x]$ if and only if for all $f(x), g(x) \in F[x]$,

$$p(x) | f(x)g(x) \Rightarrow p(x) | f(x) \text{ or } p(x) | g(x).$$

Proof. Suppose $p(x) \in F[x]$ is irreducible over $F[x]$ and that $p(x)|f(x)g(x)$.
If $p(x)\nmid f(x)$ then $gcd(p(x), f(x)) = 1$ so that $p(x)|g(x)$ by Theorem 62B on page 116.

*****

Conversely suppose,

$$p(x)|f(x)g(x) \Rightarrow p(x)|f(x) \text{ or } p(x)|g(x) \text{ for all } f(x), g(x) \in F[x].$$

We need to show $p(x)$ is irreducible or cannot be factored in $F[x]$ into polynomials of lower degree. If we state the supposition as a contrapositive statement, we have,

$$p(x)\nmid f(x) \text{ and } p(x)\nmid g(x) \Rightarrow p(x)\nmid f(x)g(x) \text{ for all } f(x), g(x) \in F[x]$$

(Note the contrapositive changes "or" to "and.")
But $p(x)\nmid f(x)g(x)$ means we cannot have $p(x) = f(x)g(x)$ for any polynomials in $F[x]$. So $p(x)$ is irreducible. □

We can now prove a fundamental result for our journey to insolvability of polynomials,

Theorem 65B. **** (Unique Factorization for Polynomials)*
Any non-constant polynomial $f(x)$ with coefficients in the field F can be expressed as an element of F times a product of monic polynomials, each of which is irreducible over the field F. This expression is unique up to order (that is, except for the order in which the factors are written).

Proof. The proof is by induction on the degree n of $f(x) \in F[x]$.
Basis Step: First we show the statement is true for $n = 1$.
Let $f(x) = a_1x + a_0$. Then $f(x) = a_1(x - a_1^{-1}a_0)$ which is an element of F times a monic irreducible polynomial, so the statement is true for $n = 1$.
Induction Step: Now suppose the statement is true for polynomials of degree $< n$. Let $f(x)$ have degree n. We need to prove $f(x)$ of degree n is the product of ireducible factors.
If $f(x)$ is irreducible, we are done. If not, let $f(x) = g(x)h(x)$ where $g(x), h(x)$ have degrees less than n, so, by the supposition, can be written as,

$$g(x) = ap_1(x)p_2(x)\dots p_j(x), \text{ of degree } r \text{ say,}$$
$$h(x) = bq_1(x)q_2(x)\dots q_k(x), \text{ of degree } n - r \text{ say,}$$

where $a, b \in F$ and all the polynomials $p_1(x), \dots, p_j(x)$ and $q_1(x), \dots, q_k(x)$ are monic and irreducible.
But then we have,

$$f(x) = g(x)h(x) = abp_1(x)p_2(x)\dots p_j(x)q_1(x)q_2(x)\dots q_k(x)),$$

of degree $n - r + r = n$, which is the product of an element of F and monic irreducible polynomials.

*****

To prove uniqueness, suppose,

$$f(x) = ap_1(x)p_2(x)\dots p_j(x) = bq_1(x)q_2(x)\dots q_k(x)$$

Clearly, $a = b$. But also, $p_1(x)|bq_1(x)q_2(x)\dots q_k(x)$ so by Theorem 64B above we must have $p_1(x)|bq_1(x)q_2(x)\cdots q_{k-1}$ or $p_1|q_k(x)$.
If $p_1(x)|q_k(x)$ then, since both are irreducible, we must have $p_1(x) = q_k(x)$. If not, we replace $p_k(x)$ with $p_{k-1}(x)$ and make the same argument. We must eventually have $p_1(x) = q_s(x)$ for some $s : 1 \le s \le k$.
We can repeat the whole process to show $p_2(x) = q_s(x)$ for some other $s : 1 \le s \le k$.
In this way we match every monic irreducible polynomial in $p_1(x)p_2(x)\dots p_j(x)$ with a monic irreducible polynomial in $q_1(x)q_2(x)\dots p_k(x)$.
There cannot be more $p_i(x)$ polynomials than $q_j(x)$ polynomials (or vice versa) since if we cancel the matched polynomials on either side of

$$p_1(x)p_2(x)\dots p_j(x) = q_1(x)q_2(x)\dots q_k(x),$$

we would be left with the product of one or more polynomials equal to 1, so they must all be 1. □

Example 57. $2x^4 + 2x^3 + 2x + 2 = 2(x+1)^2(x^2 - x + 1) \in \mathbb{Z}(x)$

8.7 Multiplicity of roots and factors

8.7.1 Integers with multiple factors

Using the Fundamental Theorem of Arithmetic, Theorem 65A, page 117, we can express any integer as,

$$n = p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}\dots p_r^{\alpha_r} = \prod_{i=1}^{r} p_i^{\alpha_i}$$

where each p_i is a prime and all $\alpha_i \in \mathbb{N}$.
Clearly, n has no multiple factors if and only if $\alpha_i \le 1$ for all i.

8.7.2 Polynomials with multiple factors

Let us now address the possibility that a polynomial has multiple factors not all distinct.

Definition 50B. *multiplicity of roots*
Let f be a field and $f(x) \in F[x]$. An element $c \in F$ is said to be a root of multiplicity $n \ge 1$ of $f(x)$ if $(x - c)$ occurs exactly n times in the unique factorization of $f(x)$.

Using Calculus[6], we prove Theorem 66B, the test for multiple roots, namely, a polynomial $f(x) \in \mathbb{R}[x]$ has no repeated factors if and only if $gcd(f(x), f'(x)) = 1$.

Theorem 66B. ** *A non-constant polynomial $f(x) \in \mathbb{R}[x]$ has no repeated factors if and only if $gcd(f(x), f'(x)) = 1$.*

Proof. Suppose $f(x)$ has no repeated factors. If,

$$f(x) = (ax + b)g(x) \text{ then } f'(x) = (ax + b)g'(x) + ag(x),$$

so that $gcd(f(x), f'(x)) = 1$.

*****

Conversely, suppose $gcd(f(x), f'(x)) = 1$.
Let $f(x)$ have a repeated factor $(ax + b)^n, n > 1$, that is,

$$f(x) = (ax + b)^n g(x) \text{ where } (ax + b) \nmid g(x)$$
$$\Rightarrow f'(x) = na(ax + b)^{n-1} g(x) + (ax + b)^n g'(x)$$

Then, $gcd(f(x), f'(x)) = (ax + b)^{n-1}$ which is a contradiction unless $n = 1$.
Hence $f(x)$ has no repeated factors. □

8.8 Tests for Roots or Factors

8.8.1 Tests for Factors of Integers

There are simple tests revealing whether an integer has the prime factors $2, 3, 5, 7, 11$ but beyond these small numbers there are no simple tests other than long division. Tests for division by 2 or 5 are trivially obvious. But, for example, a three digit number like 583 is divisible by 11 if the middle digit is the sum of the other two (e.g., $8 = 5 + 3$ so that $583 = 11 \times 53$) is not so obvious.[7] You may choose to examine divisibility by 3 (it's like the algorithm for 11) and 7 (it's trickier) before you google them.

[6] If you have not studied Calculus don't be concerned since, in the concluding chapters, we will only deal with polynomials that do not have repeated or multiple factors. This theorem simply tells us how to confirm that for any given polynomial.

[7] We can go further and show 11 is/is not a factor of larger integers by observing $10 (\text{mod } 11) \equiv -1$, $100 (\text{mod } 11) \equiv 1$, $1000 (\text{mod } 11) \equiv -1$, etc., so we have a succession of $-1, 1, -1, 1, -1, \ldots$ for powers of $10 (\text{mod } 11)$ as we work right to left on a number of any size. For example $79475 = 5 + 7 \times 10 + 4 \times 100 + 9 \times 1000 + 7 \times 10000$ makes

$$79475 \equiv -5 + 7 - 4 + 9 - 7 (\text{mod } 11) \equiv 0 (\text{mod } 11)$$

which makes 11 a factor.

8.8.2 Tests for Roots of Polynomials

Let us now consider only polynomials with integer coefficients, that is, $f(x) \in \mathbb{Z}[x]$. A simple test for rational roots is given by Theorem 67B.

Theorem 67B. ****
Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$.
If $\frac{r}{s}$ *is a rational root of* $f(x)$ *with* $gcd(r, s) = 1$, *then* $r|a_0$ *and* $s|a_n$.

Proof. If $\frac{r}{s}$ is a rational root of $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ then,

$$\begin{aligned} f\left(\frac{r}{s}\right) = 0 &\Rightarrow a_n\left(\frac{r}{s}\right)^n + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \ldots + a_1\left(\frac{r}{s}\right) + a_0 = 0 \\ &\Rightarrow a_n r^n + a_{n-1}r^{n-1}s + \ldots + a_1 r s^{n-1} + a_0 s^n = 0 \text{ (multiplying by } s^n). \\ &\Rightarrow r\left(a_n r^{n-1} + a_{n-1}r^{n-2}s + \ldots + a_1 s^{n-1}\right) = -a_0 s^n \\ &\Rightarrow r|a_0 s^n \\ &\Rightarrow r|a_0 \text{ since } gcd(r, s) = 1 \end{aligned}$$

Similarly,

$$s\left(a_{n-1}r^{n-1} + \ldots + a_1 r s^{n-2} + a_0 s^{n-1}\right) = -a_n r^n \Rightarrow s|a_n$$

□

Example 58. *The only possible rational roots of* $3x^3 + 5x^2 + 7x + 10$ *where* $a_n = 3$ *has factors* $\pm 1, \pm 3$ *and* $a_0 = 10$ *has factors* $\pm 1, \pm 2, \pm 5, \pm 10$ *are:*

$$\pm\frac{1}{1}, \pm\frac{1}{2}, \pm\frac{1}{5}, \pm\frac{1}{10}, \pm\frac{3}{1}, \pm\frac{3}{2}, \pm\frac{3}{5}, \pm\frac{3}{10}$$

Each of these can be tested by the Factor Theorem, namely Corollary 55, page 104, to find if they are actually roots.[8] ◇

8.9 Tests for Irreducibility

8.9.1 Determining whether an integer is prime

A composite number n that factors has the form $n = ab$ where a is less than or equal to the square root of the number and b is greater than or equal to the square root of the number. For example we can factor 64 as 4×16 and $\sqrt{64} = 8$ which is greater than 4 but less than 16. So if a number is not prime it must have a prime factor less than its square root, hence to test whether any given number is prime, we simply need to divide it by the primes less than its square root. If all the remainders are greater than 0 then the number is prime.

[8] Obviously a computer or sophisticated calculator can do this in less than the blink of an eye.

Example 59. *For example, consider* 191. *We have* $169 = 13^2 < 191 < 14^2 = 196$ *and the primes less than 14 are 13,11,7,5,3,2. Then,*

$$191(\text{mod}2) \equiv 1,\ 191(\text{mod}3) \equiv 2,$$
$$191(\text{mod}5) \equiv 1,\ 191(\text{mod}7) \equiv 2,$$
$$191(\text{mod}11) \equiv 4,\ 191(\text{mod}13) \equiv 9,$$

proves 191 is a prime number. ◇

In ancient times, Erasthosthenes developed a sieve to churn out primes. He wrote down a long list of the natural numbers 1,2,3, etc., skipped over 1, circled 2 as the first prime and then went through the list of natural numbers eliminating every second number after 2 (those divisible by 2). Back he went to the beginning of his list and the first number not crossed out was 3 so he crossed out every third number from 3 onwards (those divisible by 3) and so on until he reached the square root of the largest natural number he had reached in his list. (He could actually have continued to the square root of the next square above his final entry – why?) There are today some very sophisticated algorithms for finding large primes[9] but there is no formula for generating primes.

8.9.2 Determining whether a polynomial is irreducible

The obvious way to determine whether a polynomial with coefficients in $\mathbb{Z}$ is irreducible is to attempt to factor it. The key theorem is the Factor Theorem 55, page 104, which says $x - c$ is a factor of $f(x)$ if and only if $f(c) = 0$.

Example 60. *For example, if* $f(x) = x^2 - 5x - 35$ *the obvious candidates for factors are drawn from the factors of* $35 = \pm 35 \times \mp 1 = \pm 5 \times \mp 7$. *So we calculate* $f(\pm 35), f(\pm 1), f(\pm 5), f(\pm 7)$ *and find* $f(7) = f(-5) = 0$ *so that* $(x+5), (x-7)$ *are factors and* $f(x)$ *is not irreducible.* ◇

More generally, if the polynomial under consideration is not monic, say,

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0,\ a_n > 0,\ a_i \in \mathbb{Z}$$

then we have Theorem 67B, page 121, that r/s, $gcd(r, s) = 1$ is a rational root of $f(x)$ if and only if $r | a_0$ and $s | a_n$. So we only have to consider factors drawn from the factorizations of a_n and a_0. Finally, a series of lemmas, including Gauss's Lemma 68B that the product of two primitive polynomials is again primitive (where primitive means the greatest common divisor of all the coefficients is 1, or equivalently, no

[9] As of January 2017, the largest known prime number is $2^{74,207,281} - 1$, a number with 22,338,618 digits. It was found in 2016 by the Great Internet Mersenne Prime Search (GIMPS).

prime divides all the coefficients) leads, via Theorem 69B, to Eisenstein's Criterion, Theorem 70B, another essential result for us, for showing if,

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0,\ a_n > 0,\ a_i \in \mathbb{Z},$$

and there is a prime p that divides a_0 but $p^2 \nmid a_0$ and which divides all the other coefficients except a_n then $f(x)$ is irreducible over $\mathbb{Q}$.
We then have Corollary 71B that if p is a prime then the polynomial,

$$\phi(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1$$

is irreducible over the field of rational numbers. Theorem 70B and Corollary 71B give us easy access to a huge number of simple irreducible polynomials.

First a definition.

Definition D51B. *primitive polynomial*
A polynomial with integer coefficients is called primitive if the greatest common divisor of all the coefficients is 1 or, equivalently, if there is no prime p that divides all the coefficients.

Example 61. $3x^3 + 6x^2 + 5x + 7$ *is primitive but* $3x^3 + 6x^2 + 9x + 12$ *is not since 3 divides all the coefficients.*

Theorem 68B. *** (Gauss's Lemma)*
The product of two primitive polynomials is itself primitive.

Proof. Consider the two primitive polynomials,

$$f(x) = a_m x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0$$
$$g(x) = b_n x^n + b_{n-1}x^{n-1} + \ldots + b_1 x + b_0.$$

Suppose the product of these two primitive polynomials $f(x)$ and $g(x)$ is not primitive, so there exists a prime number p that is a common divisor of all the coefficients of the product. But since $f(x)$ and $g(x)$ are primitive, p cannot divide either all the coefficients of $f(x)$ or all those of $g(x)$. Let $a^r x^r$ and $b^s x^s$ be the first (i.e., highest degree) terms with a coefficient not divisible by p, respectively in $f(x)$ and in $g(x)$, that is $a_m, a_{m-1}, \ldots, a_{r+2}, a_{r+1}$ and $b_n, b_{n-1}, \ldots, b_{s+2}, b_{s+1}$ are all divisible by p.
Now consider the coefficient of x^{r+s} in the product. Its value is given by $\sum a_i b_j$, where the sum runs over all pairs of indices i, j such that $i + j = r + s$. (See Definition 46, page 100)
The coefficient of the term x^{r+s} in the product $f(x)g(x)$ is therefore,

$$a_r b_s + a_{r-1}b_{s+1} + a_{r-2}b_{s+2} + \ldots$$
$$+ b_{s-1}a_{r+1} + b_{s-2}a_{r+2} + \ldots$$

So apart from $a_r b_s$ all the other terms contain either $b_{s+1}, b_{s+2}, \ldots$ or $a_{r+1}, a_{r+2}, \ldots$ and we chose r, s so that $b_{s+1}, b_{s+2}, \ldots$ and $a_{r+1}, a_{r+2}, \ldots$ are all divisible by p, but $a_r b_s$ is not.
This contradicts the assumption that there is a prime number p that is a common divisor of all the coefficients of the product. Therefore, the coefficients of the product can have no common divisor and are thus primitive. □

Theorem 69B. ******
A polynomial with integer coefficients that can be factored into polynomials with rational coefficients can also be factored into polynomials of the same degree with integer coefficients.

Proof. Let's first understand the theorem statement using an example.
$f(x) = 6x^2 - 7x - 3$ is a polynomial with integer coefficients. It can be factored into the product of the polynomials, $6\left(x - \frac{3}{2}\right)\left(x + \frac{1}{3}\right)$ which have rational coefficients. But it can also be factored into the polynomials $(3x + 1)(2x - 3)$ with integer coefficients.

*****

Consider a polynomial with integer coefficients that can be factored into polynomials with rational coefficients, giving say,

$$\begin{aligned} f(x) &= a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0,\ a_n > 0,\ a_i \in \mathbb{Z} \\ &= (b_{1,k}x^k + b_{1,k-1}x^{k-1} + \ldots + b_{1,1}x + b_{1,0}) \ldots \\ &\qquad (b_{n,j}x^j + b_{n,j-1}x^{j-1} + \ldots + b_{n,1}x + b_{n,0}), \end{aligned}$$

where the coefficients $b_{\alpha,\beta} \in \mathbb{Q}$.
Multiplying by the product N of all the denominators of all the coefficients $b_{\alpha,\beta}$ does not affect the powers of x in any factor but it clears all the fractions in the coefficients. Extracting the product M of all the gcds of the numerators of the coefficients in all the factors also does not affect the powers of x in any factor but now all the factors are primitive polynomials with integer coefficients, say,

$$\begin{aligned} f(x) = \frac{M}{N}[(c_{1,k}x^k + c_{1,k-1}x^{k-1} + \ldots + c_{1,1}x + c_{1,0}) \cdots \\ (c_{n,j}x^j + c_{n,j-1}x^{j-1} + \ldots + c_{n,1}x + c_{n,0})], \quad c_{\alpha,\beta} \in \mathbb{Z}. \quad (8.9.1) \end{aligned}$$

where by cancellation we can assume $gcd(M, N) = 1$.
Now since $f(x)$ in its original definition has integer coefficients and $gcd(M, N) = 1$, N must divide every coefficient in the expansion of (8.9.1). But by Gauss's Lemma 67B above, the product of primitive polynomials is again primitive so N cannot be a product $N = pq$ where p is a prime, else every coefficient is divisible by p and the product is not primitive.
Therefore $N = 1$ and thus,

$$\begin{aligned} f(x) = M[(c_{1,k}x^k + c_{1,k-1}x^{k-1} + \ldots + c_{1,1}x + c_{1,0}) \ldots \\ (c_{n,j}x^j + c_{n,j-1}x^{j-1} + \ldots + c_{n,1}x + c_{n,0})],\ c_{\alpha,\beta} \in \mathbb{Z}, \end{aligned}$$

which is a factorization into factors with integer coefficients of the same degree as the factors with rational coefficients . □

Theorem 70B. ***** (Eisenstein's Irreducibility Criteria)*
Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ *be a polynomial with integer coefficients. If there exists a prime number* p *such that,*

$$a_{n-1} \equiv a_{n-2} \equiv \ldots \equiv a_0 \equiv 0 (\mathrm{mod} p)$$

that is, p *divides all of these coefficients, but* p *does not divide* a_n*, and if also* p^2 *does not divide* a_0 *then* $f(x)$ *is irreducible over* $\mathbb{Q}$*, the field of rational numbers.*

Proof. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ be a polynomial with integer coefficients and for some prime p that,

(1) $p \nmid a_n$

(2) $p | a_i$ for all $i < n$

(3) $p^2 \nmid a_0$

We will prove a contradiction by supposing $f(x)$ is reducible over $\mathbb{Q}$.
Then by Theorem 69B above, $f(x)$ factors over $\mathbb{Z}$ say,

$$f(x) = (b_j x^j + b_{j-1}x^{j-1} + \ldots + b_1 x + b_0)(c_k x^k + c_{k-1}x^{k-1} + \ldots + c_1 x + c_0) \qquad (8.9.2)$$

where the coefficients are integers and $j \neq 0, k \neq 0, j + k = n$.

The constant term in this product must be $a_0 = b_0 c_0$. Now $p^2 \nmid a_0$ means $p^2 \nmid b_0 c_0$ so that p does not divide both b_0 and c_0. But p divides $a_0 = b_0 c_0$ so p divides one of b_0 and c_0 so let's suppose $p \nmid c_0$ and $p | b_0$.
For the leading coefficients we must have $a_n = b_j c_k$. Now $p \nmid a_n = b_j c_k$ and therefore p does not divide either b_j or c_k.
Let m be the least integer for which $p \nmid b_m$, that is, $p | b_i$ for $i = 0$ to $m - 1$ but $p \nmid b_m$. We know that $1 \leq m \leq j < n$.
Now if we multiply out equation (8.9.2), we have the coefficient of x^m given by,

$$a_m = b_m c_0 + b_{m-1}c_1 + \ldots + b_1 c_{m-1} + b_0 c_m.$$

Here, for each term except the first, $p | b_i,\ i < m$, but for the first term we showed $p \nmid b_m$ and $p \nmid c_0$.
Hence $p \nmid a_m$, where $m < n$ which is contrary to condition (2). This is a contradiction to the assumption that $f(x)$ is reducible over Q.
Hence $f(x)$ is irreducible over $\mathbb{Q}$, the field of rational numbers. □

Example 62. *For example,* $f(x) = x^4 - 12x^2 + 18x - 24$ *is irreducible since* $3|12,\ 3|18,$ *and* $3|24$ *but* $3^2 \nmid 24$ *and* $3 \nmid 1 = a_4$.
Note $p = 2$ *will not prove this since* $2^2|24$. ◇

We then have Corollary 71B that if p is prime then the polynomial,

$$g(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1,$$

is irreducible over the field of rational numbers.

Note 18. *The following proof of the corollary to Eisenstein's Theorem uses the Binomial Theorem which gives the following expansion,*

$$(x+y)^n = x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \ldots + \binom{n}{n-1}xy^{n-1} + y^n$$

where $\binom{n}{k} = \dfrac{n!}{(n-k)!\ k!}$ *and* $n! = n(n-1)(n-2)\cdots 2.1$

It also uses the fact that n *divides* $\binom{n}{k}$ *for* $k \neq 0$ *or* n.

Corollary 71B. **
If p *is prime than the polynomial,*

$$g(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1,$$

is irreducible over the field of rational numbers.

Proof. Let,

$$\begin{aligned} h(x) &= g(x+1) \\ &= \frac{(x+1)^p - 1}{(x+1) - 1} \\ &= \frac{x^p + \binom{p}{1}x^{p-1} + \binom{p}{2}x^{p-2} + \ldots + px}{x} \end{aligned}$$

where the final numerator comes from the binomial theorem. Hence,

$$h(x) = x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \ldots + p$$

Then $h(x)$ satisfies the Eisenstein criteria for the prime p since, as per the conditions in the statement of Theorem 70B,

(1) $p \nmid 1$, which is the leading coeffcient,

(2) $p \mid \binom{p}{k}$ for $1 < k < p$, and $p | a_0 = p$.

(3) $p^2 \nmid a_0 = p$

and $h(x)$ is therefore irreducible over $\mathbb{Q}$.
But clearly, if $g(x) = a(x)b(x)$, then, by putting $x = x + 1$, we have that
$g(x + 1) = a(x + 1)b(x + 1)$ would also be a factorization in $\mathbb{Q}$.
Since this is not so for $h(x) = g(x + 1)$ then it cannot be so[10] for $g(x)$.
So $g(x)$ is irreducible over $\mathbb{Q}$. □

8.10 Congruence Classes

8.10.1 Congruence classes and Integers

We now redefine congruence and define congruence classes relating to $\mathbb{Z}$.

Definition 52A. *congruence for integers*
Choose a fixed $n \in \mathbb{Z}^+$. If $a, b \in \mathbb{Z}$ and $n|(a - b)$ we say a and b are congruent modulo n, written $a \equiv b(\mathrm{mod}\ n)$.
Consequently, $a - b = kn$, $k \in \mathbb{Z}$, or $a = b + kn$, or, in words, b is a remainder when a is divided by n.

Note 19. *When calculating $a \equiv b(\mathrm{mod}\ n)$ we mostly assume b is the least positive remainder when a is divided by n. Thus although,*

$$23 \equiv -2(\mathrm{mod}5),\ \ 23 \equiv 18(\mathrm{mod}5),$$
$$23 \equiv 13(\mathrm{mod}5),\ \ 23 \equiv 8(\mathrm{mod}5), \textit{etc.},$$

we usually say $23 \equiv 3(\mathrm{mod}5)$.

Let us recall our discussion in Section 5.4, page 72, of a notation for cosets.

Definition 53A. *congruence classes for integers*
Let $a \in \mathbb{Z}$, $n \in \mathbb{Z}^+$. The set of all integers that have the same remainder as a when divided by n is called the congruence class of a modulo n and is designated by $[a]_n$. That is,

$$[a]_n = \{x \in \mathbb{Z} \mid x \equiv a(\mathrm{mod}n)\}$$

Example 63. $[5]_6 = \{5, 11, 17, \ldots\} \cup \{-1, -7, -11, \ldots\}$

Notation 6. *The collection of all congruence classes modulo n is again denoted by the factor group $\mathbb{Z}/n\mathbb{Z}$, that is, (refer back to Note 16, page 83),*

$$\mathbb{Z}/n\mathbb{Z} = \{[a]_n \mid a \in \mathbb{Z},\ 0 \le a \le n - 1\} = \{[0]_n, [1]_n, \ldots, [n - 1]_n\}$$

The values of a are all the possible remainders when any integer is divided by n and are therefore given by the elements of $\mathbb{Z}_n = \{0, 1, \ldots, n - 1\}$.

[10] The proof that if $g(x)$ factors then $g(x + 1)$ factors is as follows. Let $g(x) = p(x)q(x)$. Then $g(x + 1) = p(x + 1)q(x + 1)$. So $g(x + 1)$ factors, giving the (little) theorem that if $g(x)$ factors then $g(x + 1)$ factors. The contrapositive is that if $g(x + 1)$ does not factor (as it does not here) then $g(x)$ does not factor.

Example 64. *For example, take* $n = 5$. *Then* $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$. *Thus,*

$$\mathbb{Z}/5\mathbb{Z} = \{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\} \qquad \diamond$$

8.10.2 Congruence classes and Polynomials

We now define congruence and congruence classes for polynomials $f(x) \in F[x]$ over a field F.

Definition D52B. *congruence for polynomials*
Let F *be a field and* $p(x)$ *be a fixed polynomial in* $F[x]$.
If $a(x), b(x) \in F[x]$ *and* $p(x) \mid (a(x) - b(x))$, *we say* $a(x), b(x)$ *are congruent modulo* $p(x)$, *written*

$$a(x) \equiv b(x) (\mathrm{mod} p(x))$$

Consequently, $a(x) - b(x) = p(x)q(x)$, *or* $a(x) = b(x) + p(x)q(x)$, *where* $q(x)$ *is a non-constant polynomial in* $F[x]$.

Example 65. $(x^3 + 2x) - (2x + 1) = (x - 1)(x^2 + x + 1)$ *so* $x^3 + 2x \equiv 2x - 1 (\mathrm{mod} x - 1)$

Note 20. *When calculating congruences modulo* $p(x)$ *we mostly use the polynomial of least degree. Thus although by long division on* $\dfrac{x^4 + 1}{x^2 + 1}$, *we could write,* $x^4 + 1 \equiv (-x^2 + 1) (\mathrm{mod}\ x^2 + 1)$, *we usually continue the long division to the remainder of least degree and say* $x^4 + 1 \equiv 2 (\mathrm{mod}\ x^2 + 1)$.

Definition 53B. *congruence classes for polynomials*
The set,

$$\{b(x) \in F[x] \mid a(x) \equiv b(x) (\mathrm{mod}\ p(x)\}$$

is the set of all polynomials in $F[x]$ *with the same remainder,* $a(x)$, *when divided by* $p(x)$ *and is called the congruence class of* $a(x)$ *modulo* $p(x)$ *and is denoted by* $[a(x)]_{p(x)}$.

Notation 7. *The collection of all congruence classes modulo* $p(x)$ *is denoted by the factor group* $F[x]/ < p(x) >$. *They are all the possible remainders when any polynomial in* $F[x]$ *is divided by* $p(x)$.
In Notation 5 on page 103, we defined $< g(x) >$ *to be the set of polynomials in* $F[x]$ *that are divisible by* $g(x)$. *Then we note the factor group, by Definition 33, page 71, is,*

$$\begin{aligned} F[x]/ < p(x) > &= \{(f(x) + < p(x) >) (\mathrm{mod}\ p(x)) \mid f(x) \in F[x]\} \\ &= \{(f(x) + p(x)g(x)) (\mathrm{mod}\ p(x)) \mid f(x), g(x) \in F[x]\} \\ &= \{f(x) (\mathrm{mod}\ p(x)) \mid f(x) \in F[x]\} \\ &= \{[a(x)]_{p(x)} \mid a(x) \equiv f(x) (\mathrm{mod}\ p(x)), f(x) \in F[x]\}. \end{aligned}$$

Example 66. *For example, consider* $p(x) = x^2 + 1 \in \mathbb{Z}[x]$. *The possible remainders (try the long division on some polynomials) for,*

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \ \div (x^2 + 1)$$

all have the form $ax + b,\ a, b \in \mathbb{Z}$. *Thus,*

$$F[x]/ < x^2 + 1 >= \{ax + b \mid a, b \in Z\}$$

Note this is an infinite set and also the degree of $ax + b$ *is less than the degree of* $p(x) = x^2 + 1$. ◇

We prove Theorem 72B that the congruence class $[a(x)]$ modulo $p(x)$, or simply $[a(x)]_{p(x)}$, contains a unique representative $r(x)$ with $deg(r(x)) < deg(p(x))$ or $r(x) = 0$, so that a representative polynomial of lesser degree than the divisor $p(x)$ always exists.

Theorem 72B. ***
Let $p(x) \in F[x]$, F *a field and* $p(x) \neq 0$. *Then for all* $a(x) \in F[x]$, *the congruence class*

$$[a(x)]_{p(x)} = \{b(x) \mid b(x) \equiv a(x) (\text{mod } p(x))\}$$

contains a unique representative $r(x)$ *with* $deg(r(x)) < deg(p(x))$ *or* $r(x) = 0$.

Proof. By the Division Algorithm, Theorem 57B, page 106, if $a(x) \in F[x]$, we have for some $q(x) \in F[x]$,

$$\begin{aligned} & a(x) = q(x)p(x) + r(x), \quad deg(r(x)) < deg(p(x)) \text{ or } r(x) = 0 \\ \Rightarrow\ & r(x) = a(x) - p(x)q(x) \\ \Rightarrow\ & r(x) = a(x) (\text{mod } p(x)) \\ \Rightarrow\ & r(x) \in [a(x)]_{p(x)} \end{aligned}$$

*****

To show uniqueness, we need to show if our $r(x) \in [a(x)]_{p(x)}$ and also we have an $s(x) \in [a(x)]_{p(x)}$ with $deg(s(x)) < deg(p(x))$ or $s(x) = 0$, then $s(x) = r(x)$.
Let $s(x) \in [a(x)]_{p(x)}$, then,

$$\begin{aligned} & s(x) \equiv a(x) (\text{mod } p(x)) \\ & \Rightarrow s(x) = a(x) + q_1(x)p(x) \text{ for some } q_1(x) \in F[x] \\ & (\text{Substitute for } a(x) = q(x)p(x) + r(x)) \\ & \Rightarrow s(x) = q(x)p(x) + r(x) + q_1(x)p(x) \\ & \Rightarrow s(x) - r(x) = p(x)[q(x) - q_1(x)] \\ & \Rightarrow p(x) \mid s(x) - r(x), \end{aligned}$$

which means $deg(p(x)) < deg(s(x) - r(x))$.
Since $deg(s(x) - r(x)) \leq deg(s(x))$, then $deg(p(x)) < deg(s(x))$ and this is a contradiction to $deg(s(x)) < deg(p(x))$ unless $s(x) - r(x) = 0$, that is $s(x) = r(x)$. □

8.11 Well-defined Congruency Class Definitions

8.11.1 Integers and Congruency Class Definitions

Let's revisit the coset notation and operations first met in Chapter 5.

Definition 54A. *addition and multiplication of congruence classes in $\mathbb{Z}/n\mathbb{Z}$*
We define addition and multiplication of congruence classes in $\mathbb{Z}/n\mathbb{Z}$ by,

$$[a]_n + [b]_n = [a+b]_n$$
$$[a]_n \cdot [b]_n = [a \cdot b]_n$$

Example 67.

$$[6]_7 + [4]_7 = [6+4]_7 = [10]_7 = [3]_7$$
$$[6]_7 \cdot [4]_7 = [6 \cdot 4]_7 = [24]_7 = [3]_7 \qquad \diamond$$

But we need to prove this definition makes sense, we say that it must be well-defined[11], meaning it is totally independent of the choice of a, b as the representatives of the classes $[a]_n, [b]_n$.
Accordingly, we let x, y be any other representatives of the classes $[a]_n, [b]_n$ and prove in Theorem 73A that:

$$[x+y]_n = [a+b]_n$$
$$[x \cdot y]_n = [a \cdot b]_n$$

Given these operations, it is easy to show $\mathbb{Z}/p\mathbb{Z}$, p a prime, is a commutative ring – but we can go further.

Note 21. *In general if we have,*

$$a \equiv b (\text{mod } n) \text{ then } [a]_n = [b]_n.$$

The reason is that by Definition 53A, page 127,

$$[a]_n = \{x \in \mathbb{Z} \mid x \equiv a (\text{mod } n), \text{ and}$$
$$[b]_n = \{x \in \mathbb{Z} \mid x \equiv b (\text{mod } n\}$$

Since we have $a \equiv b (\text{mod } n) \Rightarrow a = b + kn,\ k \in \mathbb{Z}$, then

$$x \equiv a (\text{mod } n) \Rightarrow x \equiv b + kn (\text{mod } n) \Rightarrow x \equiv b (\text{mod } n),$$

[11] Whether an operation is well-defined is the same idea as a function since an operation is a mapping of elements of one set onto another set. For example the square root unitary operation is $\surd : \mathbb{Z} \Rightarrow \mathbb{C}$. Just one example won't prove this, that is $\sqrt{(-9)} = 3i$ does not prove the mapping is true for all integers, we need to show the mapping holds for all $x \in \mathbb{Z}$. Hence if we make a definition of a binary operation involving two elements a, b of the first set then we need to say the definition also applies to any two other elements, say x, y, of the first set as we do here.

so,

$$\begin{aligned}[a]_n &= \{x \in \mathbb{Z} \mid x \equiv a(\text{mod } n)\} \\ &= \{x \in \mathbb{Z} \mid x \equiv b(\text{mod } n)\} \\ &= [b]_n\end{aligned}$$

Theorem 73A. ****
Let x, y be any other representatives of the classes $[a]_n, [b]_n$. Then,

$$\begin{aligned}[x+y]_n &= [a+b]_n \\ [x \cdot y]_n &= [a \cdot b]_n,\end{aligned}$$

that is the formulas do not depend upon any particular representatives of the congruency classes.

Proof. By Definition 53A on page 127,

$$[a]_n = \{x \in \mathbb{Z} \mid x \equiv a(\text{mod } n)\} = \{x \in \mathbb{Z} \mid n|(x-a)\}$$

Let x, y be any other representatives of the classes $[a]_n,\ [b]_n$. Then,

$$\begin{aligned}x \in [a]_n, y \in [b]_n &\Rightarrow x = a + kn, y = b + ln \text{ for some } k, l \in \mathbb{Z} \\ &\Rightarrow x + y = a + b + mn, \text{ where } m = k + l \\ &\Rightarrow x + y \equiv a + b(\text{mod } n) \\ &\Rightarrow [x+y]_n = [a+b]_n \text{ by Note 23, page 176}\end{aligned}$$

Also,

$$\begin{aligned}xy &= (a+kn)(b+ln) \\ &= ab + n(la + bk + kln) \\ &\Rightarrow xy = ab + mn,\ m = la + bk + kln \\ &\Rightarrow xy \equiv ab(\text{mod } n) \\ &\Rightarrow [xy]_n = [ab]_n \text{ by Note 21, page 130}\end{aligned}$$

So the formulas for addition and multiplication of congruence classes do not depend on the choice of particular representatives. We say the formulas are well defined. □

8.11.2 Polynomials and Congruency Class Definitions

Definition D54B. *addition, multiplication of congruence classes $F[x]/<p(x)>$*
Paralleling the integers, for $a(x) \in F[x]$, we denote the congruence class

$$[a(x)] \textit{ modulo } p(x) \textit{ by } [a(x)]_{p(x)}$$

and define the addition and multiplication of congruence classes in the factor group $F[x]/<p(x)>$ *by,*

$$[a(x)]_{p(x)} + [b(x)]_{p(x)} = [a(x) + b(x)]_{p(x)}$$
$$[a(x)]_{p(x)} \cdot [b(x)]_{p(x)} = [a(x) \cdot b(x)]_{p(x)}$$

Example 68.

$$\begin{aligned}[x+2]_{x^2+1} \cdot [x+4]_{x^2+1} &= [(x+2)\cdot(x+4)]_{x^2+1} \\ &= [x^2+6x+8]_{x^2+1} \\ &= [x^2+1+6x+7]_{x^2+1} \\ &= [6x+7]_{x^2+1} \qquad \diamond\end{aligned}$$

But we need to prove this definition makes sense, we say that it must be well-defined, meaning it is totally independent of the choice of $a(x), b(x)$ as representatives of the classes $[a(x)]_{p(x)}, [b(x)]_{p(x)}$.
Accordingly, we let $[c(x)]_{p(x)}, [d(x)]_{p(x)}$ be any other representatives of the classes $[a(x)]_{p(x)}, [b(x)]_{p(x)}$ and prove in Theorem 73B that,

$$[a(x)]_{p(x)} + [b(x)]_{p(x)} = [c(x)]_{p(x)} + [d(x)]_{p(x)}$$
$$[a(x)]_{p(x)} \cdot [b(x)]_{p(x)} = [c(x)]_{p(x)} \cdot [d(x)]_{p(x)}$$

Given these operations, it is easy to show $F[x]/ < p(x) >$ is a commutative ring – but we can go further.

Theorem 73B. ****
If $c(x), d(x)$ *are any other representatives of the classes* $[a(x)]_{p(x)}, [b(x)]_{p(x)}$ *then,*

$$[a(x)]_{p(x)} + [b(x)]_{p(x)} = [c(x)]_{p(x)} + [d(x)]_{p(x)}$$
$$[a(x)]_{p(x)} \cdot [b(x)]_{p(x)} = [c(x)]_{p(x)} \cdot [d(x)]_{p(x)}$$

Proof. The proof is exactly the same as the proof for the integers in Theorem 73A above by replacing

$$[a]_n \to [a(x)]_{p(x)}$$
$$[b]_n \to [b(x)]_{p(x)}$$
$$[x]_n \to [c(x)]_{p(x)}$$
$$[y]_n \to [d(x)]_{p(x)}$$

□

8.12 Multiplicative Inverses

8.12.1 Integers - Multiplicative Inverses of Congruence Classes

For the integers we prove Theorem 74A that the congruence class $[a]_n \in \mathbb{Z}/n\mathbb{Z}$ has a multiplicative inverse if and only if $gcd(a, n) = 1$.

Theorem 74A. ** *The conjugacy class $[a]_n$ has a multiplicative inverse in $\mathbb{Z}/n\mathbb{Z}$ if and only if $gcd(a, n) = 1$.*

Proof. Suppose $[a]_n$ has a multiplicative inverse $[b]_n$, Then,

$$[a]_n[b]_n = [1]_n \Rightarrow [ab]_n = [1]_n \Rightarrow ab = 1 + kn, k \in \mathbb{Z} \Rightarrow ab + (-k)n = 1$$

which by Corollary 60A, page 111, is only true when $gcd(a, n) = 1$.

*****

Conversely, suppose $gcd(a, n) = 1$. Then, by Corollary 60A, page 111,

$$\begin{aligned} & ab + kn = 1 \text{ for some } b, n \in \mathbb{Z} \\ & \Rightarrow ab \equiv 1 (\text{mod } n) \\ & \Rightarrow [ab]_n = [1]_n \textit{ by Note } \textbf{??}, \textit{page } 176 \\ & \Rightarrow [a]_n[b]_n = [1]_n \end{aligned}$$

which makes $[b]_n$ the multiplicative inverse of $[a]_n$. □

Example 69. *For example, $[5]_7 \in \mathbb{Z}/7\mathbb{Z}$ has the multiplicative inverse $[3]_7$ since*

$$[5]_7 \cdot [3]_7 = [3 \cdot 5]_7 = [15]_7 = [1]_7$$

But, noting $gcd(3, 6) \neq 1$, $[3]_6$ does not have a multiplicative inverse, since the only options are,

$$\begin{aligned} & [3]_6 \cdot [0]_6 = [0]_6, \quad [3]_6 \cdot [1]_6 = [3]_6, \quad [3]_6 \cdot [2]_6 = [0]_6 \\ & [3]_6 \cdot [3]_6 = [3]_6, \quad [3]_6 \cdot [4]_6 = [0]_6, \quad [3]_6 \cdot [5]_6 = [3]_6 \end{aligned}$$ ◇

8.12.2 Polynomials - Multiplicative Inverses of Congruence Classes

Note 22. *The following proof illustrates an "if and only if" theorem can be proved in one step using $P \Leftrightarrow Q$ rather than $P \Rightarrow Q$ and $Q \Rightarrow P$, if we can continue the "iff" to the conclusion.*

Theorem 74B. **
Let $p(x) \in F[x]$, F a field, $p(x) \neq 0$. Then any $[a(x)]_{p(x)}$ has a multiplicative inverse if and only if $gcd(a(x), p(x)) = 1$.

Proof. There is a $b[x]_{p(x)}$ such that $a[x]_{p(x)} \cdot b[x]_{p(x)} = [1]_{p(x)}$,

$$\begin{aligned}
&\Leftrightarrow [a(x)b(x)]_{p(x)} = [1]_{p(x)} \\
&\Leftrightarrow a(x)b(x) \equiv 1 (\mathrm{mod} p(x)) \\
&\Leftrightarrow a(x)b(x) = 1 + p(x)c(x) \ for\ some\ c(x) \in F[x] \\
&\Leftrightarrow a(x)b(x) - c(x)p(x) = 1.
\end{aligned}$$

But this is true if and only if $gcd(a(x), p(x)) = 1$, by Corollary 60B, page 112. □

Example 70. *For example $[ax+b]_{x^2+1}$ has the inverse $\left[\frac{-ax+b}{a^2+b^2}\right]_{x^2+1}$ since,*

$$\begin{aligned}
[ax+b]_{x^2+1} \times \left[\frac{-ax+b}{a^2+b^2}\right]_{x^2+1} &= \left[\frac{-a^2x^2+b^2}{a^2+b^2}\right]_{x^2+1} \\
&= \left[\frac{-a^2(x^2+1)}{a^2+b^2} + \frac{a^2+b^2}{a^2+b^2}\right]_{x^2+1} \\
&= \left[\frac{-a^2}{a^2+b^2}(x^2+1) + 1\right]_{x^2+1} \\
&= [1]_{x^2+1}
\end{aligned}$$

and we note $gcd(ax+b, x^2+1) = 1$. ◇

8.13 Fields

We now determine, for our later purposes, the structures involving rings of integers and polynomials that are fields.

8.13.1 Integers and Fields

As a consequence of Theorem 74A, since, as you can easily check, the missing field property is a multiplicative inverse for each of the non-zero elements, $\mathbb{Z}/p\mathbb{Z}$ is a field if and only if p is a prime number (then every congruence class has a multiplicative inverse).

Theorem 75A. *
$\mathbb{Z}/p\mathbb{Z}$ is a field if and only if p is a prime number

Proof. By Theorem 74A, page 133, the conjugacy classes $[a]_n$, $0 \leq a \leq n-1$, have a multiplicative inverse in $\mathbb{Z}/n\mathbb{Z}$ if and only if $gcd(a, n) = 1$.
But if n is not a prime then, say, $n = cd$, $0 < c, d < n-1$, then the conjugacy classes $[c]_n$

and $[d]_n$ in $\mathbb{Z}/n\mathbb{Z}$ do not have an inverse since $gcd(c, n) = c \neq 1$, and $gcd(d, n) = d \neq 1$. In turn this means their product does not have an inverse, so $\mathbb{Z}/n\mathbb{Z}$ does not have inverses.
Accordingly, since the missing Field axiom[12] is a multiplicative inverse, $\mathbb{Z}/p\mathbb{Z}$ is a field if and only if p is a prime number. □

The most interesting and important fact about $\mathbb{Z}/p\mathbb{Z}$ is that it is a finite field with just p elements.

8.13.2 Polynomials and Fields

As a consequence of Theorem 74B, since, as you can easily check, the missing property is a multiplicative inverse for each of the non-zero elements, $F[x]/ < p(x) >$ is a field if and only if $p(x)$ is irreducible in F.

Theorem 75B. *
$F[x]/ < p(x) >$ is a field if and only if $p(x)$ is irreducible in F.

Proof. By Theorem 74B, page 134, the conjugacy class $[a(x)]_{p(x)}$ has a multiplicative inverse in $F[x]/ < p(x) >$ if and only if $gcd(a(x), p(x)) = 1$.
But if $p(x)$ is reducible, say, $p(x) = c(x)d(x), deg(c(x), d(x)) > 1$, then,
the conjugacy classes $[c(x)]_{p(x)}, [d(x)]_{p(x}$ in $F[x]/ < p(x) >$ do not have an inverse since $gcd(c(x), p(x)) = c(x) \neq 1$ and $gcd(d(x), p(x)) = d(x) \neq 1$. In turn this means their product $p(x)$ will not have a multiplicative inverse.
Accordingly, since the missing field axiom[13] is a multiplicative inverse,
$F[x]/ < p(x) >$ is a field if and only if $p(x)$ is irreducible in F. □

Of course, $F[x]/ < p(x) >$ is an infinite field.

[12]The field axioms may be found in Section 7.3, page 93. You can easily check the axioms are all satisfied by $\mathbb{Z}/n\mathbb{Z}$ under coset addition and multiplication defined in Definition **??**, page **??**. The multiplicative identity is $[1]_n$.

[13]The field axioms may be found in Section 7.3, page 93. You can easily check the axioms are all satisfied by $F[x]/<p(x)>$ under coset addition and multiplication defined in Definition **??**, page **??**. The multiplicative identity is $[1]_{p(x)}$.

Chapter 9

Fields I

9.1 Preamble

9.1.1 Field Extensions

Our goal is to prove the insolvability of polynomials of degree ≥ 5 by radicals. Having obtained the results we need for the ring of polynomials, we turn our attention to fields and field extensions.

We define an extension field F of a (base) field K if K is a subset of F and K is a field under the same operations as apply to F. We use the symbol F/K to mean K is a subfield of F or, equivalently, F is an extension field of K.

For example $\mathbb{C}$ is an extension field of $\mathbb{R}$ since both are fields under the ordinary operations of addition and multiplication (excepting 0 from both for multiplication). Actually $\mathbb{C}$ is $\mathbb{R}$ with the addition of $i = \sqrt{-1}$ or $\mathbb{C} = \mathbb{R}(i)$ spoken as
"$\mathbb{C}$ is $\mathbb{R}$ append i."

We continue our study of polynomials with coefficients in any general base field in which addition and multiplication are defined. We again use the symbol $K[x]$ for polynomials in the variable x with coefficients in the field K. We found the polynomials in $K[x]$ form a commutative ring with identity. In particular, we consider $K = \mathbb{Q}$ and the ring of polynomials $\mathbb{Q}[x]$.

******

Our goal is to find, where possible, the solutions of polynomial equations with coefficients in $\mathbb{Q}$. The process begins with building a tower of fields, each a subset of the "higher" one. We proceed as follows. After we have found one solution or root, α, of our polynomial $f(x) \in \mathbb{Q}$, that is $f(\alpha) = 0$, we construct the extension field $F = \mathbb{Q}(\alpha)$ over $\mathbb{Q}$. Since the polynomial has a root in $F = \mathbb{Q}(\alpha)$, it can be factored into polynomials of lesser degree with coefficients in $F = \mathbb{Q}(\alpha)$. Then each of the factors of this lower degree polynomial are investigated similarly until a field is obtained which is the smallest field inside $\mathbb{Q}$ that contains $\mathbb{Q}$ and all the roots of $f(x)$.

Example 71. *For example, if* $f(x) = x^4 - 5x^2 + 6 = (x^2 - 2)(x^2 - 3)$, *one factor is* $(x - \sqrt{2})$ *so one root is* $\sqrt{2}$ *and we can write,*

$$f(x) = (x - \sqrt{2})g(x), \quad g(x) = x^3 + \sqrt{2}x^2 - 3x - 3\sqrt{2}$$

where $g(x)$ *is clearly of lesser degree (3) than* $f(x)$ *and has coefficients in the extension field* $\mathbb{Q}(\sqrt{2})$ *of* $\mathbb{Q}$.
Then we factor $g(x) = x^3 + \sqrt{2}x^2 - 3x - 3\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ *into*

$$g(x) = (x + \sqrt{2})(x^2 - 3) = (x + \sqrt{2})(x + \sqrt{3})(x - \sqrt{3})$$

The root $\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ *but the roots* $\pm\sqrt{3}$ *do not. So we construct a further extension field*[1] $\mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
Then all the roots of $f(x) = (x - \sqrt{2})(x + \sqrt{2})(x - \sqrt{3})(x + \sqrt{3})$ *lie in this extension. The tower of fields we created was,*

$$\begin{array}{c} \mathbb{Q}(\sqrt{2}, \sqrt{3}) \\ | \\ \mathbb{Q}(\sqrt{2}) \\ | \\ \mathbb{Q} \end{array}$$

For another example, consider,

$$f(x) = x^4 - x^3 - 2 = (x^2 - 2)(x^2 + 1) = (x - \sqrt{2})(x + \sqrt{2})(x - i)(x + i)$$

Here we would need the tower,

$$\begin{array}{c} \mathbb{C} \\ | \\ \mathbb{Q}(\sqrt{2}, i) = \{c + d\sqrt{2}i \mid c, d \in \mathbb{Q}(\sqrt{2}) \\ | \\ \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}) \\ | \\ \mathbb{Q} \end{array}$$

◇

The key question is when can we build such a tower of fields and extension fields? A secondary question is how are the tiers in the tower related?

[1] In general we claim $F(a)(b) = F(a, b)$. We prove double containment.
$F(a, b)$ is the smallest field containing F, a and b. Obviously $F(a)(b)$ contains F, a and b also so it must be a bigger field or an equal field, that is $F(a, b) \subseteq F(a)(b)$.
But in general $F(c)$ is the smallest field containing c and therefore $F(a, b)$ is the smallest field containing F, a and b. So, since $F(a)(b)$ also contains F, a and b, it must be a bigger field or an equal field giving $F(a)(b) \subseteq F(a, b)$, so by double containment we have $F(a)(b) = F(a, b)$.

First we prove that if u_1 is a solution of the polynomial equation $f(x) = 0$ where $f(x) \in K[x]$, then we can form an extension field F of K namely $F = K(u_1)$. We call such a u_1 an algebraic number.

Then if $f(x) = a_n(x-u_1)(x-u_2)\cdots(x-u_n)$, since $f(u_1) = f(u_2) = \ldots f(u_n) = 0$, we conclude we can form the extension fields, $F = K(u_1, u_2)$, $F = K(u_1, u_2, u_3), \ldots$, and finally, $F = K(u_1, u_2, \ldots, u_n)$ in which $f(x)$ "splits" or can be factored into a product of linear factors.

Hence we call $F = K(u_1, u_2, \ldots, u_n)$ a splitting field for $f(x)$ over K.

9.1.2 Minimal polynomials

We proceed to prove that for any element u in the extension field F of K that there exists a unique monic polynomial, $p(x)$, of least degree, such that $p(u) = 0$. We call $p(x)$ the minimal polynomial of the algebraic number[2] u. It is these minimal polynomials that form the links between the tiers of the tower – and in what we will find is a very simple manner.

We review the introductory theory of vector spaces before proceeding. After that we prove that if $F = K[u]$ is an extension field of K and $u \in F$ is algebraic over K with minimal polynomial of degree n, then $K(u)$ is an n–dimensional vector space over K.

We define the dimension[3] of F as a vector space over K as the degree of F over K and denote it by $[F : K]$. Then we show $[F : K]$ is the degree of the minimal polynomial $p(x)$ of $u \in F$ where $F = K(u)$. We prove every element of a finite extension must be algebraic. For the tower of fields and subfields,

$$\begin{array}{c} \mathrm{F} \\ | \\ \mathrm{E} \\ | \\ \mathrm{K} \end{array}$$

we prove that,

$$[F : K] = [F : E][E : K]$$

This makes life simple in a case such as,

$$\begin{array}{c} \mathbb{Q}(u_1, u_2) \\ | \\ \mathbb{Q}(u_1) \\ | \\ \mathbb{Q} \end{array}$$

[2]Given F/K, $u \in F$ is an algebraic number if it is a root of a polynomial with coefficients in K.

[3]The dimension of a vector space is the number of vectors in any basis. We will review vector theory below.

We simply need to find the degrees of the minimal polynomials, $p_1(x), p_2(x)$ of u_1, u_2 respectively, say n_1, n_2, and then the degree of F over K, or the number of vectors in any basis, is $[F : K] = n_1 n_2$.

9.1.3 Galois Groups and Extension Fields

Let's recall that the elements of the symmetric group S_n are functions that act on $\{1, 2, 3, \ldots, n\}$ and permute their order. We want to relate permutations of the finite number of roots, $u_1, u_2, \ldots, u_n$, in the factoring of $f(x)$ in an extension field to the permutations of S_n of acting on $\{1, 2, \ldots, n\}$.

We begin by defining the parallel functions that will permute the roots of $f(x)$. We call them automorphisms. We define an automorphism acting on a field as a one-to-one correspondence, $\phi : F \to F$, that maps elements of the field onto other elements of the same field, meaning $\phi(a) = c$ where both $a, c \in F$, and ϕ is also a field homomorphism. That is, for all $a, b \in F$ we have,

$$\begin{aligned} \phi(ab) &= \phi(a)\phi(b) \\ \phi(a+b) &= \phi(a) + \phi(b) \end{aligned}$$

In other words an automorphism is an isomorphism mapping a field onto itself. We use the notation, $Aut(F) = \{\phi \mid \phi : F \to F, \phi \text{ is an isomorphism}\}$.

We define the Galois group of the extension field F/K as the group of automorphisms of F that fix the elements of K, hence,

$$Gal(F/K) = \{\phi \in Aut(F) \mid \phi(a) = a \text{ for all } a \in K\}$$

after, of course, we first prove it is a group (under the operation of composition of functions as for S_n).

Then we make the definition that if $f(x) \in K[x]$ splits in F so that $F = K(u_1, u_2, \ldots, u_n)$ where $f(x) = a_n(x - u_1)(x - u_2)\cdots(x - u_n)$ then $Gal(F/K$ is called the Galois group of $f(x)$ over K.

Again, in line with our desire for comparability with the elements of S_n, we prove any element of $Gal(F/K)$ permutes the roots $\{u_1, u_2, \ldots, u_n\}$ of $f(x)$ in F just as any element of S_n permutes the elements in $\{1, 2, \ldots, \}$.

A simple example of the Galois group of a polynomial in $\mathbb{Q}[x]$ is obtained as follows.

$$\begin{aligned} f(x) &= x^3 - 1 \\ &= (x-1)(x^2 + x + 1) \\ &= (x-1)(x-\omega)(x+\omega^2), \ \omega = -\frac{1}{2} + \frac{\sqrt{3}i}{2} \end{aligned}$$

The Galois group whose elements leave the rational roots unchanged but permute the roots ω, ω^2 has just two elements, the first being the identity function and the

second a simple interchange:

$$\phi_1(\omega) = \omega,\ \phi_1(\omega^2) = \omega^2$$
$$\phi_2(\omega) = \omega^2,\ \phi_2(\omega^2) = \omega$$

The next question is how many elements can there be in the Galois group, $Gal(F/K)$? The answer is simple. We prove it is the degree of F as a vector space over K, that is,

$$|Gal(F/K)| = [F : K]$$

9.1.4 Fundamental Theorem of Galois Theory

Our next goal is to prove the Fundamental Theorem of Galois Theory. We first prove that for a field F and a subgroup G of $Aut(F)$ that the elements in F that are fixed by every element of G form a subfield of F which we label F^G and call the G–fixed subfield of F, the notation being,

$$F^G = \{a \in F \mid \phi(a) = a \text{ for all } \phi \in G\}$$

If $G = Gal(F/K)$ and F is the splitting field of a separable[4] polynomial, then we prove the fixed subfield is actually the base field K, that is, $F^G = K$.

We proceed to prove that if F is a splitting field for $f(x)$ over K and $f(x)$ is separable with no repeated roots, then if $p(x)$ is the minimal polynomial of any element of F it must be that $p(x)$ splits into linear factors in F. This means that F is a splitting field for any and every irreducible polynomial in $K[x]$ that has a root in F. We say F is a normal or Galois extension of K.

To put it all together, we say F is a Galois extension of K or F is Galois over K if it is a finite, normal, separable extension of K, which is always the case if F is simply the splitting field of a separable polynomial with no multiple roots.

So now we have it all set up. We have a tower of fields and subfields built up from the roots of a separable polynomial $f(x) \in K[x]$ and we have a group, $Gal(F/K)$ of functions that permute the n roots of $f(x)$ that lie in the extension field F, paralleling the elements of the symmetric group, S_n, that permute the set of integers, $\{1, 2, \ldots, n\}$. And just as S_n has subgroups, so to does $Gal(F/K)$, so both have a finite chain of subgroups like,

$$\{e\} < G_1 < G_2 < \ldots < G_n = G.$$

Finally we prove the Fundamental Theorem of Galois Theory, that there is a reversing correspondence between the tower of fields and the chain of subgroups and we find what this correspondence is.

[4] A separable polynomial has no multiple roots.

9.1.5 Insolvability of Degree ≥ 5 Polynomials

Which brings us to our goal, to prove the quintic, and all polynomials of degree ≥ 5, are not solvable by radicals.

This means there is, for them, no formula involving the operations $+, -, \times, \div$ or taking n^{th} roots, for finding the roots of ALL polynomials of degree ≥ 5.

We begin by defining an extension field, F, to be a radical extension of a base field K if there exist elements $u_1, u_2, \ldots, u_m \in F$ such that $F = K(u_1, u_2, \ldots, u_m)$ and we can build a tower of subfields and fields between K and F by applying the conditions $u_1^{n_1} \in K$ and $u_i^{n_i} \in K(u_1, u_2, \ldots, u_{i-1})$ for $i = 2, 3, \ldots, m$ and $n_1, n_2, \ldots, n_m \in \mathbb{Z}$.

In essence, each extension field contains one more n^{th} root of one of the elements $u_1, u_2, \ldots u_m \in F$ like this,

$$
\begin{array}{c}
F = K(u_1, u_2, \ldots, u_m) \\
| \\
u_m^{n_m} \in K(u_1, u_2, \ldots, u_{m-1}) \\
| \\
\vdots \\
| \\
u_3^{n_3} \in K(u_1, u_2) \\
| \\
u_2^{n_2} \in K(u_1) \\
| \\
u_1^{n_1} \in K
\end{array}
\qquad \diamond
$$

We make the definition that $f(x) \in K[x]$ is solvable by radicals if there exists a radical extension F of K that contains all the roots of $f(x)$.

We proceed to prove the main theorem, Galois' masterpiece, that we need to show the quintic and polynomials of higher degree are not solvable by radicals. The theorem states "Given $f(x) \in K[x]$, if the equation $f(x) = 0$ is solvable by radicals then the Galois group of $f(x)$ over K is solvable."

The contrapositive statement of this theorem is all we need, it states "Given $f(x) \in K[x]$, if the Galois group of $f(x)$ over K is not solvable, then the equation $f(x) = 0$ is not solvable by radicals."

Using group theory theorems we proceed to find a polynomial $f(x)$ of degree 5 whose Galois group of permutations is actually S_5. Then since $S_n,\ n \geq 5$ is not solvable, neither is the polynomial equation $f(x) = 0$ solvable by radicals. The same argument applies to polynomials of higher degree.

9.2 Extension Fields and Polynomials

Let us begin.

Definition 55. *field extension*
A field F is an extension field of a field K if K is a subset of F and is a field under the same two operations as F.

Notation 8. *field extension*
If F is an extension field of K we write F/K.

We first need to show extension fields exist with the required conditions applying to them. We prove Kronecker's Theorem 76 that for K a field and any non-constant polynomial $f(x) \in K[x]$ that there exists an extension field F of K and an element $u \in F$ such that $f(u) = 0$.

Theorem 76. **** (Kronecker)*
Let K be a field and $f(x)$ be any non-constant polynomial in $K[x]$. Then there exists an extension field F of K and an element $u \in F$ such that $f(u) = 0$.

Proof. Let K be a field and $f(x)$ be any non-constant polynomial in $K[x]$.
By Theorem 65B, page 118, the polynomial $f(x)$ can be written as the product of irreducible factors. Let $p(x)$ be any one of the irreducible factors of $f(x)$ so that $f(x) = p(x)g(x)$, say. We need only find an extension field F of K containing an element u such that $p(u) = 0$ making $f(u) = p(u)g(u) = 0$.
By Theorem 75B, page 135, $F = K[x]/ < p(x) >= \{a(x)+ < p(x) > \mid a(x) \in K[x]\}$ is a field.
We claim $G = \{a+ < p(x) > | a \in K\}$ is a subfield of F isomorphic to K.
Since we are dealing with fields, the subfield test is that for subgroups under the two operations of addition and multiplication. Accordingly, $G \subseteq F$ is a subfield of F only,

- If $a+ < p(x) >, b+ < p(x) > \in G$ then $a+ < p(x) - (b+ < p(x) >) \in G$. This is true since,[5]

$$\begin{aligned} a+ < p(x) > -(b+ < p(x) >) &= a+ < p(x) > -b- < p(x) > \\ &= a-b+ < p(x) > \in G \text{ since } a-b \in K. \end{aligned}$$

- If $a+ < p(x) >, b+ < p(x) > \in G$ then $(a+ < p(x) >)(b+ < p(x) >)^{-1} \in G$.
  This is true since $b+ < p(x) > \in G < F$ means $b+ < p(x) > \in F$.
  But F is a field so the inverse of $b+ < p(x) > \in F$.
  Now $(b+ < p(x) >)(b^{-1}+ < p(x) >) = bb^{-1}+ < p(x) >= 1+ < p(x) >$ so the inverse of $b+ < p(x) >$ is $b^{-1}+ < p(x) >$. Then,

$$(a+ < p(x))(b^{-1}+ < p(x) >) = ab^{-1}+ < p(x) \in G \text{ since } ab^{-1} \in K.$$

[5]Note $< p(x) >$ is a group as shown in Notation 5 on page 103.

Hence $G = \{a + < p(x) > | a \in K\}$ is a subfield of F.

*****

To show $K \cong G$, we can define the map,

$$\psi : K \to G \text{ where } \psi(a) = a + < p(x) >$$

We now prove ψ is an isomorphism of these two fields. By Definition 47, page 103, we must prove it is,

1. One-to-one: We must prove $\psi(a) = \psi(b) \Rightarrow a = b$.
   Suppose $\psi(a) = \psi(b)$. Then $a+<p(x)>= b+<p(x)> \Rightarrow a = b$.

2. Onto: We must prove for every $\psi(a) = a+<p(x)>$ there is a corresponding element in K, namely a. But that is obvious.

3. A field homomorphism: We must prove ψ is a homomorphism under both of the operations, addition and multiplication. We have,

$$\begin{aligned} \psi(a+b) &= a+b+<p(x)>= a+<p(x)>+b+<p(x)>= \psi(a)+\psi(b) \\ \psi(ab) &= ab+<p(x)>= (a+<p(x)>)(b+<p(x)>) = \psi(a)\psi(b) \end{aligned}$$

Note, in the expansion of $\psi(a+b)$ and $\psi(ab)$ since $< p(x) >$ is a group, we can say[6]

$$\begin{aligned} a* <p(x)>= b* <p(x)>=<p(x)> \\ <p(x)> * <p(x)>=<p(x)>, \end{aligned}$$

where $* = \times \text{ or } +$.
So ψ is an isomorphism and we have $K \cong G$. Now as we proved above, G is a subfield of F so, using the isomorphism, we can regard $F = K[x]/<p(x)>$ as an extension field of K which proves the first statement.

*****

Finally, we must show $F = K[x]/<p(x)>$, the set of all congruence classes modulo $p(x)$, contains a congruence class that is a zero of $p(x)$.
Let $p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ and consider the conguence class $[x]_{p(x)} = x \in F$. Then,

$$\begin{aligned} p([x]_{p(x)}) &= a_n[x]^n_{p(x)} + a_{n-1}[x]^{n-1}_{p(x)} + \ldots + a_1[x]_{p(x)} + a_0 \\ &= [a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0]_{p(x)} \\ &= [p(x)]_{p(x)} \\ &= 0 \end{aligned}$$

So F contains a zero of $p(x)$, namely the congruence class $[x]_{p(x)}$. □

[6]See, for example, Note 13, page 70

Example 72. *Consider* $f(x) = x^2 + 1 \in \mathbb{Q}[x]$.
Since $x^2 + 1 = (x + i)(x - i)$ *the extension field of* $\mathbb{Q}$ *is* $\mathbb{Q}(i)$ *and* $i \in \mathbb{Q}(i)$ *with* $f(i) = i^2 + 1 = 0$. $\diamond$

Extending Kronecker's Theorem leads to the proof of Corollary 77 that there exists an extension field F of K over which $f(x)$ can be factored into a product of linear factors.

Corollary 77. **
Let K *be a field and* $f(x)$ *be any non-constant polynomial in* $K[x]$. *Then there exists an extension field* F *of* K *over which* $f(x)$ *can be factored into linear factors (factors of the type* $(x - c)$*).*

Proof. We build a series of extension fields as follows. First, we factor out the k linear factors of $f(x)$ in $K[x]$, leaving $f(x) = (a_1x - b_1)(a_2x - b_2)\cdots(a_kx - b_k)g_1(x)$. Here, if it exists, $g_1(x)$ is irreducible in $K[x]$ and $deg(g_1(x)) > 1$. Note also that the k roots $\frac{b_i}{a_i}$ of $f(x)$ all lie in K and therefore in any extension field.
Then we apply Theorem 76, page 142, to find an extension field F_1 containing a root u_1 of $g_1(x)$ so we have

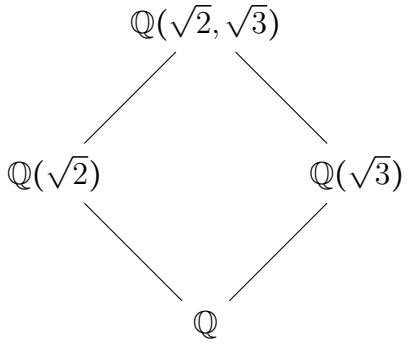
$$f(x) = (a_1x - b_1)(a_2x - b_2)\cdots(a_kx - b_k)(x - u_1)g_2(x)$$

Then we again apply Theorem 76 to find an extension field F_2 containing a root u_2 of $g_2(x)$ to obtain,

$$f(x) = (a_1x - b_1)(a_2x - b_2)\cdots(a_kx - b_k)(x - u_1)(x - u_2)g_3(x)$$

We continue in this way until we have an extension field F containing all the roots of $f(x)$. $\square$

Example 73. *Pictorially, we have for* $f(x) = x^4 - 5x^2 + 6 = (x^2 - 2)(x^2 - 3)$ *the lattice of two towers of extension fields of the base field* $\mathbb{Q}$ *as follows,*



$\diamond$

Let us now revisit algebraic numbers.

9.3 Algebraic Numbers

Definition 56. *algebraic numbers*
Given an extension field F of a base field K we say $u \in F$ is an algebraic number over K if there exists a non-zero polynomial $f(x) \in K[x]$ such that $f(u) = 0$. More simply, such a $u \in F$ is said to be algebraic over K.

Example 74. *For example, in the tower of fields above, both $\sqrt{2}$ and $\sqrt{3}$ are algebraic over $\mathbb{Q}$ since they are the roots of the respective polynomials $f(x) = x^2 - 2$ and $g(x) = x^2 - 3$ with coefficients in $\mathbb{Q}$.* $\diamond$

9.4 Monic minimal polynomials

In Theorem 78 we extend Kronecker's Theorem 76 to prove that if F is an extension field of K and $u \in F$ then there exists a unique monic polynomial $p(x) \in K[x]$ such that $p(u) = 0$. It is characterized as the monic polynomial of minimal degree that has u as a root.

Example 75. *Now $\frac{-1+\sqrt{3}i}{2} \in \mathbb{Q}(\sqrt{3}, i)$ which is an extension field of $\mathbb{Q}$. We claim there exists a unique monic polynomial $p(x) \in \mathbb{Q}[x]$ such that $p\left(\frac{-1+\sqrt{3}i}{2}\right) = 0$, and there is, namely $p(x) = x^2 + x + 1$ which has roots $\frac{-1 \pm \sqrt{3}i}{2}$* $\diamond$

There are two possibilities for the elements $u \in F$. One is $u \in K$ and the monic polynomial is $p(x) = x - u$; the other is $u \notin K$ but only $u \in F$. We are then looking for a polynomial that factors in F but not in K. An example is $f(x) = x^2 + 1 \in \mathbb{Q}[x]$, which is irreducible in $K = \mathbb{Q}$ but not in the extension field $F = \mathbb{Q}(i)$, since there $f(x)$ factors as $(x + i)(x - i)$.
Furthermore, we also prove in Theorem 78 that if $f(x)$ is any polynomial in $K[x]$ with $f(u) = 0$ then $p(x) \mid f(x)$, justifying its characterization as the minimal polynomial.

Theorem 78. ******
Let F be an extension field of K and let $u \in F$ be algebraic over K. Then there exists a unique monic irreducible polynomial $p(x) \in K[x]$ such that $p(u) = 0$. It is the monic polynomial of minimal degree that has u as a root. Furthermore, if $f(x)$ is any polynomial in $K[x]$ with $f(u) = 0$ then $p(x) \mid f(x)$.

Proof. We have four statements to prove.

1. $p(x)$ exists
   If $u \in F$ is an algebraic number and thus a root of some nonzero polynomial $f(x) \in F[x]$, let $p(x)$ have the smallest or minimal degree of all the polynomials of which u is a root. So $p(x)$ exists since we have at least one polynomial with u as a root, namely $f(x)$.

2. $p(x) \mid f(x)$.
   By the Division Algorithm, Theorem 57B, page 106, we can write,
   $$f(x) = q(x)p(x) + r(x),\ r(x) = 0 \text{ or } deg(r(x)) < deg(p(x))$$
   Then,
   $$r(x) = f(x) - q(x)p(x) \Rightarrow r(u) = f(u) - q(u)p(u) = 0$$
   But if we have $r(u) = 0$ and $deg(r(x)) < deg(p(x))$ then this contradicts the choice of $p(x)$ with minimal degree such that $p(u) = 0$ unless $r(x) = 0$ which means,
   $$f(x) = q(x)p(x) \Rightarrow p(x) \mid f(x).$$

3. $p(x)$ is irreducible.
   Further, let $p(x) = g(x)h(x)$ where $g(x), h(x) \in K[x]$, so we are assuming $p(x)$ may be reducible to a product of polynomials of lesser degree.
   Substituting $x = u$ gives $g(u)h(u) = p(u) = 0 \Rightarrow g(u) = 0$ or $h(u) = 0$, but again, since the degrees of $g(x), h(x)$ are less than the degree of $p(x)$, this contradicts $p(x)$ as the polynomial of minimal degree of which u is a root or $p(u) = 0$. So $p(x)$ is irreducible.

4. $p(x)$ is unique.
   Suppose $p(x), q(x)$ both have the same degree and $p(u) = 0, q(u) = 0$. Let,
   $$p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$
   $$q(x) = b_n x^n + b_{n-1}x^{n-1} + \ldots + b_1 x + b_0$$
   Then,
   $$\begin{aligned} 0 &= p(u) - q(u) \\ &= u^n(a_n - b_n) + u^{n-1}(a_{n-1} - b_{n-1}) + \ldots + u(a_1 - b_1) + (a_0 - b_0) \end{aligned}$$
   Since $u \neq 0$, this is impossible unless $a_i - b_i = 0$ for $0 \leq i \leq n$ and then all $a_i = b_i \Rightarrow p(x) = q(x)$.

□

Example 76. *The polynomial $f(x) = x^4 + 3x^2 + 2$ satisfies $f(i) = i^4 + 3i^2 + 2 = 0$. Then the unique monic polynomial of i which is $p(x) = x^2 + 1$ must divide $f(x)$. Indeed,*
$$f(x) = x^4 + 3x^2 + 2 = (x^2 + 2)(x^2 + 1). \qquad \diamond$$

Definition 57. *minimal polynomial*
In Theorem 84 we proved that if F is an extension field of K and $u \in F$ is algebraic over K, then there exists a unique monic polynomial $p(x) \in K[x]$ such that $p(u) = 0$. This $p(x)$ is the monic polynomial of minimal degree that has u as a root. We define this $p(x)$ as the minimal polynomial of u over K and its degree is called the degree of u over K.

Example 77. *In our tower of extension fields above, we had $K = \mathbb{Q}$ and the extension field $F = \mathbb{Q}(\sqrt{2})$. Then there exists a unique monic polynomial $p(x) \in \mathbb{Q}[x]$ such that $p(\sqrt{2}) = 0$, namely $p(x) = x - \sqrt{2}$ and we note that any other polynomial that has $\sqrt{2}$ as a root such as,*

$$f(x) = x^4 - 5x^2 + 6 = (x^2 - 2)(x^2 - 3) = (x - \sqrt{2})(x + \sqrt{2})(x - \sqrt{3})(x + \sqrt{3})$$

is divisible by $p(x) = x - \sqrt{2}$ as it clearly is, since one of its factors is $(x - \sqrt{2})$. $\diamond$

In our tower of fields above, $f(x) = x^4 - 5x^2 + 6$ had four roots, $\pm\sqrt{2}, \pm\sqrt{3}$, so we begin to extend our definitions to cover the whole tower.

Definition 58. *extension field generated by $u_1, u_2, \ldots, u_n$*
We say if F is an extension field of K and $u_1, u_2, \ldots, u_n \in F$ then the smallest subfield of F that contains K and $u_1, u_2, \ldots, u_n$ is called the extension field of K generated by $u_1, u_2, \ldots, u_n$, written $F = K(u_1, u_2, \ldots, u_n)$.

Definition 59. *simple extension*
If $F = K(u)$ for a single element $u \in F$ then F is said to be a simple extension of K.

We use the Fundamental Theorem of Ring Homomorphisms (Theorem 44) to prove Theorem 79.

Theorem 79. ******
Let F be an extension field of K and let $u \in F$. If u is algebraic over K, then we have the isomorphism of fields given by $K(u) \cong K[x]/ < p(x) >$, where $p(x)$ is the minimal polynomial of u over K.

Proof. Define $\phi : K[x] \to K[u]$ by $\phi(f(x)) = f(u)$ for all polynomials $f(x) \in K[x]$. In other words,

$$\begin{aligned} f(x) &= a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \\ \Rightarrow \phi(f(x)) &= a_n u^n + a_{n-1}u^{n-1} + \ldots + a_1 u + a_0 \end{aligned}$$

Then ϕ is a ring homomorphism since,

$$\begin{aligned} \phi(f(x)g(x)) &= f(u)g(u) = \phi(f(x))\phi(g(x)) \\ \phi(f(x) + g(x)) &= f(u) + g(u) = \phi(f(x)) + \phi(g(x)) \end{aligned}$$

Now let's apply the Ring Homomorphism Theorem 44, page 92. Note since ϕ is clearly onto, then as shown in Note 17, page 103, the image of ϕ is all of $K[u]$.
We need to identify $ker(\phi) = \{f(x) \in K[x] \mid f(u) = 0\}$. Since u is algebraic over K, the minimal polynomial $p(x)$ of u over K, by Theorem 84, page 158, divides all $f(x) \in K[x]$.
Hence, $ker(\phi) =< p(x) >$, the set of all polynomials divisible by $p(x)$.
We conclude that by the Ring Homomorphism Theorem that,

$$K[x]/ < p(x) > \cong K[u]$$

But, by Theorem 75B on page 135, $K[x]/ < p(x) >$ is a field and therefore so is $K[u]$. Since $K(u)$ is clearly the smallest subfield of F containing K and u, then $K(u)$ is contained within any other subfield, so $K(u) \subset K[u]$.
But $K[u] = \{a_n u^n + a_{n-1}u^{n-1} + \ldots + a_1 u + a_0 \mid a_i \in K\}$ and each of these elements is contained in $K(u)$ so that $K[u] \subset K(u)$.
By double containment, we have $K(u) = K[u]$ and hence,

$$K[x]/ < p(x) > \cong K(u)$$

□

Finally we prove in Theorem 80 a restatement of Kronecker's Theorem 76, page 142, that if $p(x)$ is any irreducible polynomial in $K[x], K$ a field, then there exists an extension field F of K and an element $u \in F$ such that $p(x)$ is the minimal polynomial of u over K.

Theorem 80. ***
Let K be a field and $p(x) \in K[x]$ be any irreducible polynomial. Then there exists an extension field F of K and an element $u \in F$ such that the minimal polynomial of u over K is $p(x)$.

Proof. This is just Kronecker's Theorem 76 restated with $f(x)$ replaced by $p(x)$. □

We next unfold the theory of finite fields and algebraic extensions. We need an introductory understanding of vector spaces.

9.5 Vector Spaces

Vector spaces are defined in introductory courses on linear algebra. We will stay in three dimensions or $\mathbb{R}^3$ but the arguments apply to any number of dimensions or $\mathbb{R}^n$ in general.
In three dimensions, the point (2,4,3) may be regarded as the vector (arrow) drawn from the origin (0,0,0) to the point (2,4,3) and also referred to simply as the vector (2,4,3). We add vectors such as (x_1, x_2, x_3) by adding their respective x_1, x_2, x_3 values thus,

$$(1, 2, 3) + (4, 5, 6) = (5, 7, 9)$$

We can multiply a vector by any real number (in general, by a scalar) by multiplying each x, y, z in turn by it, thus,

$$5(1, 2, 3) = (5, 10, 15)$$

The $\mathbb{R}^n$ vector space is an $n-$dimensional space "full" of vectors of the form

$$(x_1, x_2, \ldots, x_n),\ x \in \mathbb{R}$$

Definition 60. *basis*
A basis $\mathfrak{B}$ of a vector space is a set of vectors which can be put together in a linear equation[7] *to form any given vector.*

Example 78. *For example, in the third dimension, $\mathbb{R}^3$, one basis is the set of vectors,*

$$\{(1,0,0),(0,1,0),(0,0,1)\},$$

since any other vector can be reformatted into a linear equation using only elements from this set and scalars from (in this case), $\mathbb{R}$. For example,

$$(4,5,-6) = 4(1,0,0) + 5(0,1,0) - 6(0,0,1) \qquad \diamond$$

Definition 61. *spans*
A set of vectors spans a vector space if every vector in the space can be written as a linear combination of those vectors.

Example 79. *For example, we say the set $\{(1,0,0),(0,1,0),(0,0,1)\}$ spans $\mathbb{R}^3$ since any vector (x_1,x_2,x_3) can obviously be written as,*

$$(x_1,x_2,x_3) = x_1(1,0,0) + x_2(0,1,0) + x_3(0,0,1)$$

Or, to put it another way, any point in $\mathbb{R}^3$, can be "reached" from the origin through a linear combination of the elements of the basis. $\diamond$

There are obviously many bases for a given vector space. In $\mathbb{R}^3$ we could also use,

$$\mathfrak{B} = \{(7,0,0),(0,-8,0),(0,0,29)\}$$

since,

$$(x_1,x_2,x_3) = \frac{x_1}{7}(7,0,0) + \frac{x_2}{-8}(0,-8,0) + \frac{x_3}{29}(0,0,29)$$

But we cannot choose just any set of three vectors for a basis. Let's see why not.

Definition 62. *linear independence*
We say the basis vectors must be linearly independent, meaning, for $\mathbb{R}^3$ that,

$$\{(a,b,c),(d,e,f),(g,h,i)\}$$

is a basis only if any linear combination of them is only trivially zero, that is, for all scalars p,q,r it is NEVER the case that,

$$p(a,b,c) + q(d,e,f,) + r(g,h,i) = (0,0,0)$$

unless $p = 0, q = 0, r = 0$.

[7] Hence linear algebra

Example 80. *For example, in* $\mathbb{R}^3$, *the set* $\{(-1,0,1),(2,1,3),(0,1,5)\}$ *is not a basis since we can form,*

$$2(-1,0,1)+(2,1,3)-(0,1,5)=(0,0,0)$$

and the coefficients $\{2,1,-1\}$ *are not all zero. What this means graphically is that you cannot find every point in* $\mathbb{R}^3$ *through a linear combination of these three vectors. For example, you cannot "reach"* $(4,3,8)$*since we cannot solve the required equations:*

$$p(-1,0,1)+q(2,1,3)+r(0,1,5)=(4,3,8) \tag{9.5.1}$$
$$\Rightarrow -p+2q+0r=4 \tag{9.5.2}$$
$$0p+q+r=3 \tag{9.5.3}$$
$$p+3q+5r=8 \tag{9.5.4}$$

since $(9.5.2)+(9.5.4)$ *yields* $5q+5r=12\Rightarrow q+r=\dfrac{12}{5}$ *whereas* $(9.5.3)$ *says* $q+r=3$. ◇

Definition 63. *dimension of a vector space*

The number of vectors in the basis of a vector space is called the dimension of the vector space. (We have not proved all bases contain the same number of vectors, but that is so.)

Let us now generalize since we want to use polynomials and not points in $\mathbb{R}^n$ as our vectors. We use script $\mathfrak{letters}$ for vectors.

Definition 64. *vector space axioms*
Let F *be a field. A vector space over* F *is a set* V *with a binary operation* $+$ *defined for all vectors* $\mathfrak{u},\mathfrak{v},\mathfrak{w}\in V$ *and a scalar product* $a\mathfrak{v}\in V$ *for all* $a\in F$ *such that the following axioms hold for all* $\mathfrak{u},\mathfrak{v},\mathfrak{w}\in V$ *and* $a,b\in F$.

(1) $\mathfrak{u}+\mathfrak{v}\in V$

(2) $(\mathfrak{u}+\mathfrak{v})+\mathfrak{w}=\mathfrak{u}+(\mathfrak{v}+\mathfrak{w})$

(3) $\mathfrak{o}\in V$ *such that* $\mathfrak{o}+\mathfrak{v}=\mathfrak{v}$

(4) For each $\mathfrak{v}\in V$ *there is a* $-\mathfrak{v}$ *such that* $-\mathfrak{v}+\mathfrak{v}=\mathfrak{o}$

(5) $\mathfrak{u}+\mathfrak{v}=\mathfrak{v}+\mathfrak{u}$

(6) $a\mathfrak{v}\in V$

(7) $a(b\mathfrak{v})=(ab)\mathfrak{v}$

(8) $(a+b)\mathfrak{v}=a\mathfrak{v}+b\mathfrak{v}$

(9) $a(\mathfrak{u} + \mathfrak{v}) = a\mathfrak{u} + a\mathfrak{v}$

(10) $1\mathfrak{v} = v$

For any field F, $F[x]$ is a vector space over F where addition of polynomials is ordinary addition of polynomials in $F[x]$ and scalar multiplication of an element of $F[x]$ by an element of F is ordinary multiplication in $F[x]$. The 10 axioms can be readily validated. Here are two of them,

$$(5) f(x) + g(x) = g(x) + f(x) \text{ for all } f(x), g(x) \in F[x]$$
$$(8)(a + b)f(x) = af(x) + bf(x) \text{ for all } f(x) \in F[x] \text{ and } a, b \in F.$$

Further, if F is an extension field of K then F is a vector space over K where addition of vectors is the usual addition in F and scalar multiplication is the usual field multiplication in F with $a \in K$ and the vector $\mathfrak{u} \in F$. Note the field of scalars is actually a subset of the field of vectors.

Our previous definitions remain the same, namely,

- A set of vectors **spans** the vector space if every other vector can be written as a linear combination (using scalars from F) of them.
  For example, if K is a field and F is an extension field of K then let $u \in F$ be algebraic over K. Then $K(u)$ is a vector space over K with basis $(1, u, u^2, \ldots, u^{n-1})$ where $n = [K(u) : K]$ is the degree of u over K as we prove below in Theorem 87.

- A **basis** of a vector space is a set of vectors that span the vector space and are linearly independent, that is any linear combination of them is never 0 unless all the scalars involved are 0.

- The **dimension** of a vector space is the number of vectors in any basis.

Chapter 10

Fields II

Algebraic Extension Fields and Splitting Fields

10.1 Algebraic Extension Fields

Definition 65. *algebraic extension field*
An extension field of F over K is an algebraic extension field if every element of F is algebraic over K meaning every element of F is the root of a polynomial with coefficients in K.

Let us now continue our investigation of polynomials with roots in algebraic extension fields. We immediately use our knowledge of vector spaces.

Definition 66. *dimension of an extension field as a vector space*
The dimension of a vector space is the number of elements in any basis. In general if F is an extension field of K then the dimension of F as a vector space over K is called the degree of F over K and we denote it by the symbol $[F : K]$.

We first prove in Theorem 81 that for an extension field F/K, with $u \in F$ an element algebraic over K, that if the minimal polynomial[1] of u over K has degree n then $K(u)$ is an $n-$dimensional vector space over K, that is $[K(u) : K] = n$, with basis $\mathfrak{B} = \{1, u, u^2, \ldots, u^{n-1}\}$.

Theorem 81. *****
Let F be an extension field of K and let $u \in F$ be an element algebraic over K. If the minimal polynomial of u over K has degree n then $K(u)$ is an $n-$dimensional vector space over K, or $[K(u) : K] = n$, and basis $\mathfrak{B} = \{1, u, u^2, \ldots, u^{n-1}\}$.

Proof. Let $p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ be the minimal polynomial of u over K.
By Theorem 79, page 147, $K(u) \cong K[x]/ < p(x) >$

[1] Definition 57, page 146

Now the cosets of $K[x]/ < p(x) >$ are the remainders when all $f(x) \in K[x]$ are divided by the minimal polynomial $p(x)$. Since $p(x)$ has degree n the remainders have at most degree $n-1$. Hence,

$$K[x]/ < p(x) >= \{a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1x + a_0 \mid a_i \in K\}$$

Accordingly, using the isomorphism, $K(u) \cong K[x]/ < p(x) >$,

$$K(u) = \{a_{n-1}u^{n-1} + a_{n-2}u^{n-2} + \ldots + a_1u + a_0 \mid a_i \in K\}$$

Thus a basis for $K(u)$ as a vector space over K is,

$$\mathfrak{B} = \{1, u, u^2, ..., u^{n-1}\}$$

which spans $K(u)$ since any element of $K(u)$ is a linear combination of these elements. Also $\mathfrak{B}$ is a linearly independent set of vectors since,

$$\begin{aligned} &a_{n-1}u^{n-1} + a_{n-2}u^{n-2} + \ldots + a_1u + a_0 = 0 \\ &\Rightarrow p(u) - a_nu^n = 0 \\ &\Rightarrow a_nx^n = 0, \text{ since } p(u) = 0 \end{aligned}$$

But $u^n \neq 0$ and $a_n \neq 0$ so we cannot have $a_{n-1}u^{n-1} + a_{n-2}u^{n-2} + \ldots + a_1u + a_0 = 0$ unless each $a_i = 0$ which is the definition of linear independence.
By Definition 66, page 152, $[K(u) : K] = |\mathfrak{B}| = n$ which is the degree of $p(x)$. □

Example 81. *For example, $i \in \mathbb{Q}(i)$ is algebraic over $\mathbb{Q}$. Its minimal polynomial in $\mathbb{Q}[x]$ is $p(x) = x^2 + 1$ which has degree 2.*
We claim $\mathbb{Q}(i)$ is a 2-dimensional vector space which is easily seen to be the case since $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q},\ b \neq 0\}$. So a basis for $\mathbb{Q}(i)$ is $\{1, i\}$ since any element in $\mathbb{Q}(i)$ is a linear combination $a * 1 + b * i = a + bi, a, b \in \mathbb{Q}$ of these two elements.
We also need to show $1, i$ are linearly independent, that is, $a+bi = 0$ if and only if $a = 0$ and $b = 0$. We can simply solve $a + bi = 0 \Rightarrow a = -bi \Rightarrow a^2 = -b^2$, which is impossible unless $a = b = 0$, which is the definition of linear independence. ◇

Put simply, if F is an extension field of K and $u \in F$ is algebraic over K then $[F : K]$ is the degree of the minimal polynomial of u.

Example 82. *For example, consider $\mathbb{Q}(\sqrt{2})$ as an extension field of $\mathbb{Q}$. The minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $p(x) = x^2 - 2$ which has degree 2 and clearly $\sqrt{2}$ is algebraic over $\mathbb{Q}$ since it is the root of a monic polynomial with coefficients in $\mathbb{Q}$. Also $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ so that a basis for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}(\sqrt{2})$ is $\mathfrak{B} = \{1, \sqrt{2}\}$ thus $|\mathfrak{B}| = 2$, making $[\mathbb{Q}(\sqrt{2} : \mathbb{Q}] = 2$ also.* ◇

We proceed to prove in Theorem 82 that every element of a finite extension must be algebraic.

Theorem 82. *****
Let F be an extension field of K and let $u \in F$. TFAE or the following conditions are equivalent:

(1) u is algebraic over K.

(2) $K(u)$ is a finite extension of K.

(3) u belongs to a finite extension of K.

Proof. (1) $\Rightarrow$ (2)
If u is algebraic over K then u is the root of a polynomial with coefficients in K. Since such a polynomial necessarily has finite degree any extension containing all its roots is finite.
(2) $\Rightarrow$ (3)
Obvious.
(3) $\Rightarrow$ (1).
We need to show any u in any finite extension of K is an algebraic number, that is it is the root of a polynomial with coefficients in K.
Suppose $u \in F$, F an extension field of K and $[F : K] = n$. We showed in Theorem 81 above that the set $\{1, u, u^2, ..., u^{n-1}\}$ is a basis for $K(u)$ as a vector space over K. Therefore any vector is a linear combination of the elements of this set and not all the coefficients can be zero. Specifically, the vector u^n must be,

$$u^n = a_0 + a_1 u + \ldots + a_{n-1} u^{n-1}, \ a_i \in K$$
$$\Rightarrow a_0 + a_1 u + \ldots + a_{n-1} u^{n-1} - a_n u^n = 0$$

and not all the $a_i's$ can be zero. Therefore u is algebraic over K since it is the solution of $f(x) = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} - a_n x^n$. □

We will be building towers of finite extensions like this as we did above,

$$\begin{array}{c} \mathbb{Q}(u_1, u_2) \\ | \\ \mathbb{Q}(u_1) \\ | \\ \mathbb{Q} \end{array}$$

and using the formula proved below in Theorem 83, that if E is a finite extension of K and F is a finite extension of E then F is a finite extension of K and
$[F : K] = [F : E][E : K]$.

Theorem 83. ******
Let E be a finite extension of K and F be a finite extension of E. Then F is a finite extension of K and $[F : K] = [F : E][E : K]$.

Proof. Let E be a finite extension of K and F be a finite extension of E, thus:

$$\begin{array}{c} F \\ | \\ E \\ | \\ K \end{array}$$

Let $[F : E] = n$, $[E : K] = m$. Let $u_1, u_2, \ldots, u_n$ be a basis for F over E and let $v_1, v_2, \ldots, v_m$ be a basis for E over K. Consider,

$$\begin{aligned} \mathfrak{B} &= \{u_i v_j \mid 1 \le i \le n,\ 1 \le j \le m\} \\ &= \{u_1 v_1, u_1 v_2, \ldots, u_1 v_m, \\ &\qquad u_2 v_1, u_2 v_2, \ldots, u_2 v_m, \\ &\qquad \ldots \\ &\qquad u_n v_1, u_n v_2, \ldots, u_n v_m, \} \end{aligned}$$

This set has n rows and m elements per row, so $|\mathfrak{B}| = nm$. We will prove $\mathfrak{B}$ is a basis for F over K so that $[F : K] = |\mathfrak{B}| = mn = [F : E][E : K]$.
We need to show $\mathfrak{B}$ spans F over K, that is every vector in F can be written as a linear combination of the elements of $\mathfrak{B}$. and that the vectors in $\mathfrak{B}$ are linearly independent.

*****

First, the linear combinations for any vector $u \in F$.
If $\{u_1, u_2, \ldots, u_n\}$ is a basis for F over E and $\{v_1, v_2, \ldots, v_m\}$ is a basis for E over K then any element $u \in F$ is given by,

$$u = a_1 u_1 + a_2 u_2 + \ldots + a_n u_n$$

where each $a_i \in E$ so that,

$$a_i = c_{i1} v_1 + c_{i2} v_2 + \ldots + c_{im} v_m,\ c_{ij} \in K.$$

Thus,

$$\begin{aligned} u &= c_{11} u_1 v_1 + c_{12} u_1 v_2 + \ldots + c_{1m} u_1 v_m \\ &\quad + c_{21} u_2 v_1 + c_{22} u_2 v_2 + \ldots + c_{2m} u_2 v_m \\ &\quad + \ldots \\ &\quad + c_{n1} u_n v_1 + c_{n2} u_n v_2 + \ldots + c_{nm} u_n v_m \end{aligned}$$

so that u is a linear combination of the elements of $\mathfrak{B}$ and hence $\mathfrak{B}$ spans F over K.

*****

Second, to prove linear independence we need to prove any linear combination of the basis elements is zero only if all the coefficients in the linear combination are zero. Suppose,

$$\begin{aligned}
&c_{11}u_1v_1 + c_{12}u_1v_2 + \ldots + c_{1m}u_1v_m \\
&+ c_{21}u_2v_1 + c_{22}u_2v_2 + \ldots + c_{2m}u_2v_m \\
&+ \ldots \\
&+ c_{n1}u_nv_1 + c_{n2}u_nv_2 + \ldots + c_{nm}u_nv_m = 0
\end{aligned}$$

Replacing rows with columns, we can re-order the terms thus,

$$\begin{aligned}
&(c_{11}u_1 + c_{21}u_2 + \ldots + c_{n1}u_n)v_1 \\
&+ (c_{12}u_1 + c_{22}u_2 + \ldots + c_{n2}u_n)v_2 \\
&+ \ldots \\
&+ (c_{1m}u_1 + c_{2m}u_2 + \ldots + c_{nm}u_n)v_m = 0
\end{aligned}$$

Since the elements $\{v_1, v_2, \ldots, v_m\}$ form a basis for E over K and are therefore linearly independent, each of the coefficients $c_{1j}u_1 + c_{2j}u_2 + \ldots + c_{nj}u_n$, $1 \le j \le m$, (which belong to F) must be zero. Then since the elements $\{u_1, u_2, \ldots, u_n\}$ are a basis for F over E, for each i we must have $c_{ij} = 0$ for all j. This proves $\mathfrak{B}$ is a linearly independent set. Thus,

$$[F : K] = |\mathfrak{B}| = nm = [F : E][E : K].$$

□

Example 83. *Consider*
$f(x) = x^4 - 5x^2 + 6$.
As we "ascend" the tower of extension fields from $\mathbb{Q}$ *to* $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ *we have,*

$$\begin{array}{rl}
 & \mathbb{Q}(\sqrt{2}, \sqrt{3}) \\
p_2(x) = x^2 - 3,\ deg\ 2 & \Big| \\
 & \mathbb{Q}(\sqrt{2} \\
p_1(x) = x^2 - 2,\ deg\ 2 & \Big| \\
 & \mathbb{Q}
\end{array}$$

Thus, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] \times [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \times 2 = 4$ *since the respective degrees of the minimal polynomials are* $2, 2$.

Since,

$$\begin{aligned}\mathbb{Q}(\sqrt{2}) &= \{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\} \text{ and}\\ \mathbb{Q}(\sqrt{2},\sqrt{3}) &= \{x+y\sqrt{3} \mid x,y \in \mathbb{Q}(\sqrt{2})\}\\ &= \{a+b\sqrt{2}+(c+d\sqrt{2})\sqrt{3} \mid a,b,c,d \in \mathbb{Q}\}\\ &= \{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \mid a,b,c,d \in \mathbb{Q}\},\end{aligned}$$

a basis for $\mathbb{Q}(\sqrt{2},\sqrt{3})$ *is* $\mathfrak{B} = \{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$ *and hence,*

$$[\mathbb{Q}(\sqrt{2},\sqrt{3})] = |\mathfrak{B}| = 4 = [\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})] \times [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \qquad \diamond$$

10.2 Splitting Fields

Let's return to the discussion of polynomials over K and their roots in an extension field F/K. Let us keep in mind that we want to build a tower of fields above a base field $K = \mathbb{Q}$ for polynomials $f(x) \in K[x]$ where each extension field contains one or more of the roots of $f(x)$ that do not lie in K.

We have seen in Kronecker's Theorem 76 that given any field and any polynomial over that field that there exists an extension field in which the polynomial has a root. We extend this finding by defining the concept of a splitting field which contains all the roots of the polynomial.

Definition 67. *splitting field*
Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ *be a polynomial in* $K[x]$ *of degree* $n > 0$. *An extension field* F/K *is called a splitting field for* $f(x)$ *over* K *if there exist elements* $r_1, r_2, \ldots, r_n \in F$ *such that* $f(x) = a_n(x-r_1)(x-r_2)\cdots(x-r_n)$ *and* $F = K(r_1, r_2, \ldots, r_n)$. *In this case, we say* $f(x)$ *splits over* F. *In simple terms,* $f(x)$ *has a splitting field* F *over* K *if it factors in* F *into the product of linear factors (such as* $(x-\sqrt{2})$*).*

Example 84. *For example, let* $K = \mathbb{Q}$ *and consider*

$$\begin{aligned}f(x) &= x^4 - 5x^2 + 6\\ &= (x-\sqrt{2})(x+\sqrt{2})(x-\sqrt{3})(x+\sqrt{3})\end{aligned}$$

Then $F = \mathbb{Q}(\sqrt{2},\sqrt{3})$ *is a splitting field for* $f(x)$ *over* $\mathbb{Q}$. $\diamond$

We proceed to prove in Theorem 84 that if $f(x) \in K[x]$ is a polynomial of degree $n > 0$ then there exists a splitting field F for $f(x)$ over K with $[F : K] \leq n!$

Theorem 84. ******
Let $f(x) \in K[x]$ be a polynomial of degree $n \geq 0$. Then there exists a splitting field F for $f(x)$ over K, with $[F : K] \leq n!$

Proof. The proof is by induction on the degree of $f(x)$.
Basis Step: If $deg(f(x)) = 1 \Rightarrow f(x) = a(x - b)$, then K itself is a splitting field and $[K : K] = 1 \leq 1!$
Induction Step: Assume the theorem is true for any polynomial $g(x) \in K[x]$ with $deg(g(x)) < n$.
We need to prove $f(x)$ with degree n splits over K. Let $p(x)$ be an irreducible factor of $f(x)$, so $f(x) = p(x)q(x)$ for some $q(x) \in K[x]$.
By Kronecker's Theorem 76, page 142, there exists an extension field E of K in which $p(x)$ has a root r. Since $g(x)$ is any polynomial in $K[x]$ consider $K(r)$ with $g(x) \in K(r)[x]$, that is $g(x)$ has its coefficients in $K(r)$. We have the tower,

$$\begin{array}{c} F \\ | \\ K(r) \\ | \\ K \end{array}$$

Over the field $K(r)$, $f(x)$ factors as,

$$f(x) = p(x)q(x) = (x - r)g(x)$$

for our chosen polynomial $g(x)$, $deg(g(x)) = n - 1$.
Thus, by the induction hypothesis there exists a splitting field F of $g(x)$ over $K(r)$. By definition this means if (say) $g(x) = b(x - r_1)(x - r_2)\cdots(x - r_{n-1})$ then this splitting field is

$$F = K(r_1, \ldots, r_{n-1})$$

and, again by the hypothesis, $[F : K(r)] \leq (n - 1)!$
We are done since it is clear that

$$f(x) = b(x - r)(x - r_1)(x - r_2)\cdots(x - r_{n-1}),\ deg(f(x)) = n,$$

splits or has all its roots in the extension field.

$$F = K(r)(r_1, \ldots, r_{n-1}) = K(r, r_1, \ldots, r_{n-1})$$

Finally, note $[K(r) : K] \leq n$ since the irreducible minimal polynomial $p(x)$ has degree at most the degree of $f(x)$ which is n.
Then, by Theorem 83, page 154,

$$[F : K] = [F : K(r)] \times [K(r) : K] \leq (n - 1)!n = n!$$

□

Example 85. *Consider the splitting field of* $f(x) = x^3 - 1$ *over* $\mathbb{Q}$. *Now,*

$$\begin{aligned} f(x) = 0 &\Rightarrow x^3 - 1 = 0 \\ &\Rightarrow (x - \sqrt[3]{2})(x - \omega\sqrt[3]{2})(x - \omega^2\sqrt[3]{2}) = 0,\ \omega = -\frac{1}{2} + \frac{\sqrt{3}i}{2} \end{aligned}$$

As we noted earlier, ω *is a root of the monic polynomial* $x^2 + x + 1$ *which is irreducible in* $\mathbb{Q}$ *so our tower of fields with monic polynomials is,*

$$\begin{array}{rc} & \mathbb{Q}(\sqrt[3]{2}, \omega) \\ p_2(x) = x^2 + x + 1,\ deg\ 2 & \Big| \\ & \mathbb{Q}(\sqrt[3]{2}) \\ p_1(x) = x^3 - 2,\ deg\ 3 & \Big| \\ & \mathbb{Q} \end{array}$$

Hence,

$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ *and* $[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt[3]{2})] = 2 \Longrightarrow [\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q})] = 6 \leq 3!$ ⋄

Chapter 11

Galois Groups of Polynomials

11.1 Galois Group

In Section 2.3 we saw two examples of groups formed by the roots of polynomials. The Galois groups will consist of functions that permute the roots of polynomials. The functions will be automorphisms.

Definition 68. *automorphism on a field*
An automorphism on a field F is a one-to-one and onto function (a one-to-one correspondence[1]) $\phi : F \to F$, such that for all $a, b \in F$,

$$\phi(ab) = \phi(a)\phi(b)$$
$$\phi(a + b) = \phi(a) + \phi(b)$$

In other words, an automorphism is a field isomorphism that maps a field onto itself in the sense that any element of the field maps to another element of the field.

Notation 9. *We use $Aut(F)$ for the set of all automorphisms of F.*

In what follows we will always have F as an extension field of a field K and a polynomial $f(x) \in K[x]$. Again, for our purposes, $K = \mathbb{Q}$. We first prove in Theorem 85 that the subset of automorphisms of F defined by,

$$G = \{\phi \in Aut(F) \mid \phi(a) = a \text{ for all } a \in K\}$$

is a group under composition of functions. We say these are the automorphisms that "fix" K, in the sense that they may alter or permute elements of F that are not in K but they leave the elements of K unaltered.

[1]Recall, a one-to-one correspondence is a one-to-one and onto function, and the simple way to remember the definition of a one-to-one correspondence between the elements of two sets is that it is a function where every element of the first set is paired with exactly one element of the second set and every element of the second set is paired with exactly one element of the first set.

Theorem 85. ** *Let F be an extension field of a field K. The set of all automorphisms,*

$$G = \{\phi : F \to F \mid \phi(a) = a \quad for\ all\ a \in K\}$$

is a group under composition of functions.

Proof. Let $G = \{\phi : F \to F \mid \phi(a) = a \ for\ all\ a \in F\}$. We use the subgroup test, Corollary 3, page 31, namely if $\phi, \psi \in G$ then we need to show $\phi\psi^{-1} \in G$.
Let $\phi, \psi \in G$ so that $\phi(a) = a, \psi(a) = a$ for all $a \in K$, then,

$$\begin{aligned}\phi\psi^{-1}(a) &= \phi(\psi^{-1}(a)) \\ &= \phi(\psi^{-1}(\psi(a)) \text{ since } \psi(a) = a \\ &= \phi(a) \text{ since } \psi^{-1}\psi(a) = a \\ &= a \text{ since } \phi(a) = a\end{aligned}$$

Then $\phi\psi^{-1} \in G$ since it "fixes" $a \in K$.
Therefore, by the subgroup test, we have the subgroup

$$\{\phi \in Aut(F) \mid \phi(a) = a \ for\ all\ a \in F\} \text{ of } Aut(F).$$

□

It is the set of automorphisms of Theorem 85 that are fundamental to our goal. They merit the name of Galois.

Definition 69. *Galois group of an extension field*
We define the Galois group of F over K, denoted by $Gal(F/K)$, by,

$$Gal(F/K) = \{\phi \in Aut(F) \mid \phi(a) = a \text{ for all } a \in K\}$$

In words, the Galois group of an extension field over the base field is the set of automorphisms that fix all the elements of the base field.

Definition 70. *Galois group of a polynomial*
If the extension field F of a base field K is the splitting field of a polynomial $f(x) \in K[x]$, that is $F = K(r_1, r_2, \ldots, r_n)$ for the polynomial,

$$\begin{aligned}f(x) &= a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \\ &= a_n(x - r_1)(x - r_2)\cdots(x - r_n),\ r_i \neq r_j \text{ for all } i, j \text{ such that } 1 \leq i, j \leq n,\end{aligned}$$

then $Gal(F/K)$ is called the Galois group of $f(x)$ over K.

We now prove that if F is an extension field of K and $f(x) \in K[x]$ then any element of the Galois group $Gal(F/K)$ permutes or rearranges the roots of $f(x)$ that lie in F (paralleling the permutations of S_n that permute the elements of $\{1, 2, \ldots, n\}$.)

Theorem 86. *****
Let F be an extension field of K and let $f(x) \in K[x]$. Then any element of $Gal(F/K)$ defines a permutation of the roots of $f(x)$ that lie in F.

Proof. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ where $a_i \in K$ for $1 \leq i \leq n$.
If $u \in F$ with $f(u) = 0$ and $\phi \in Gal(F/K)$ then, using the properties of an isomorphism (note, an automorphism is also an isomorphism), and, by definition of the Galois group, that $\phi(a_i) = a_i$ for $1 \leq i \leq n$, we have,

$$\begin{aligned}
\phi(f(u)) &= \phi(a_n u^n + a_{n-1}u^{n-1} + \ldots + a_1 u + a_0) \\
&= \phi(a_n u^n) + \phi(a_{n-1}u^{n-1}) + \ldots + \phi(a_1 u) + \phi(a_0) \\
&= \phi(a_n)\phi(u^n) + \phi(a_{n-1})\phi(u^{n-1}) + \ldots + \phi(a_1)\phi(u) + \phi(a_0) \\
&= a_n\phi(u)^n + a_{n-1}\phi(u)^{n-1} + \ldots + a_1\phi(u) + a_0 \\
&= f(\phi(u))
\end{aligned}$$

Now $f(u) = 0 \Rightarrow \phi(f(u)) = \phi(0) = 0$ and therefore $f(\phi(u)) = 0$.
In other words, if u is a root of $f(x)$ then so is $\phi(u)$. This means ϕ maps roots of $f(x)$ onto roots of $f(x)$. Since there are only finitely many roots and ϕ is a one-to-one correspondence, ϕ must define a permutation of those roots of $f(x)$ that lie in F. □

11.2 The Size of the Galois Group

Our next goal is to prove that if K is a field and F is a splitting field for a polynomial $f(x) \in K[x]$ then the size of the Galois group $Gal(F/K)$ is given by,

$$|Gal(F/K)| = [F : K]$$

where $|Gal(F/K)|$ is the number of automorphisms in the Galois Group and $[F : K]$ is the dimension of F as a vector space over K.
In the cases that interest us, this is a simple formula for the number of automorphisms in the Galois group of $f(x)$ over K, since if F is an extension field of K and $u \in F$ is algebraic over K with minimal polynomial of degree n then $[F : K]$ is equal to the degree n of the minimal polynomial of F over K so that the number of automorphisms in the Galois group is simply n. We prove this challenging series of theorems and then the desired corollary.

Theorem 87. ******
Let $\theta : K \to L$ be an isomorphism of fields.
Let F be an extension field of K such that $F = K(u)$ for some algebraic element $u \in F$.
Let $p(x)$ be the minimal polynomial of u over K.
Let v be any root of the image $q(x)$ of $p(x)$ under θ, that is $\theta(p(x)) = q(x)$ and $q(v) = 0$, and let $E = L(v)$.
Then there is a unique way to extend $\theta : K \to L$ to an isomorphism $\phi : F \to E$ such that $\phi(u) = v$ and $\phi(a) = \theta(a)$ for all $a \in K$.
Diagrammatically, this means we have,

$$\begin{array}{ccc} F = K(u) & \xrightarrow{\phi} & E = L(v) \\ {\scriptstyle p(x)}\Big| & & \Big|{\scriptstyle q(x)} \\ K & \xrightarrow{\theta} & L \end{array}$$

Proof. Let $\theta : K \to L$ be an isomorphism of fields.
Let F be an extension field of K such that $F = K(u)$ for some algebraic element $u \in F$.
Let $p(x)$ be the minimal polynomial of u over K.
Let v be any root of the image $q(x)$ of $p(x)$ under θ, that is $\theta(p(x)) = q(x)$ and $q(v) = 0$, and let $E = L(v)$.
Now, by Theorem 81, page 152, if $p(x)$ has degree n, a basis for F as a vector space over K is $\mathfrak{B} = \{1, u, u^2, \ldots, u^{n-1}\}$ so that the elements of $K(u)$ have the form,

$$a_{n-1}u^{n-1} + a_{n-2}u^{n-2} + \ldots + a_1u + a_0, \ a_i \in K.$$

Therefore we define the required field isomorphism $\phi : K(u) \to L(v)$ by,

$$\phi(a_{n-1}u^{n-1} + a_{n-2}u^{n-2} + \ldots + a_1u + a_0) = \theta(a_{n-1}v^{n-1} + a_{n-2}v^{n-2} + \ldots + a_1v + a_0)$$

Clearly ϕ is a one-to-one correspondence.
But, by Definition 47, page 103, we need to show ϕ is a field isomorphism obeying both the sum and product requirement, that is, if $f(x), g(x) \in K[x]$, then,

$$\phi(f(x) + g(x)) = \phi(f(x)) + \phi(g(x)) \text{ and } \phi(f(x)g(x)) = \phi(f(x))\phi(g(x))$$

Let $f(u), g(u) \in K(u)$ be such that,

$$\begin{aligned} f(u) &= a_{n-1}u^{n-1} + a_{n-2}u^{n-2} + \ldots + a_1u + a_0 \\ g(u) &= b_{n-1}u^{n-1} + b_{n-2}u^{n-2} + \ldots + b_1u + b_0 \end{aligned}$$

We use the fact that θ is a field isomorphism.

$$\begin{aligned}
&\phi(f(u)+g(u))\\
&=\phi(a_{n-1}u^{n-1}+a_{n-2}u^{n-2}+\ldots+a_1u+a_0+b_{n-1}u^{n-1}+b_{n-2}u^{n-2}+\ldots+b_1u+b_0)\\
&=\theta(a_{n-1}v^{n-1}+a_{n-2}v^{n-2}+\ldots+a_1v+a_0+b_{n-1}v^{n-1}+b_{n-2}v^{n-2}+\ldots+b_1v+b_0)\\
&=\theta(a_{n-1}v^{n-1}+a_{n-2}v^{n-2}+\ldots+a_1v+a_0)+\theta(b_{n-1}v^{n-1}+b_{n-2}v^{n-2}+\ldots+b_1v+b_0)\\
&\quad\text{(since } \theta \text{ is an isomorphism)}\\
&=\phi(a_{n-1}u^{n-1}+a_{n-2}u^{n-2}+\ldots+a_1u+a_0)+\phi(b_{n-1}v^{n-1}+b_{n-2}v^{n-2}+\ldots+b_1v+b_0)\\
&=\phi(f(u))+\phi(g(u))
\end{aligned}$$

Second,

$$\begin{aligned}
&\phi(f(u)\cdot g(u))\\
&=\phi((a_{n-1}u^{n-1}+a_{n-2}u^{n-2}+\ldots+a_1u+a_0)\cdot(b_{n-1}u^{n-1}+b_{n-2}u^{n-2}+\ldots+b_1u+b_0))\\
&=\phi(a_{n-1}b_{n-1}u^{2n-2}+\ldots+\sum_{i+j=k}a_ib_ju^k+\cdots+a_0b_0)\\
&=\theta(a_{n-1}b_{n-1}v^{2n-2}+\ldots+\sum_{i+j=k}a_ib_jv^k+\cdots+a_0b_0)\\
&=\theta((a_{n-1}v^{n-1}+a_{n-2}v^{n-2}+\ldots+a_1v+a_0)\cdot(b_{n-1}v^{n-1}+b_{n-2}v^{n-2}+\ldots+b_1v+b_0))\\
&=\theta(a_{n-1}v^{n-1}+a_{n-2}v^{n-2}+\ldots+a_1v+a_0)\cdot\theta(b_{n-1}v^{n-1}+b_{n-2}v^{n-2}+\ldots+b_1v+b_0)\\
&=\phi(a_{n-1}u^{n-1}+a_{n-2}u^{n-2}+\ldots+a_1u+a_0)\cdot\phi(b_{n-1}u^{n-1}+b_{n-2}u^{n-2}+\ldots+b_1u+b_0)\\
&=\phi(f(u))\cdot\phi(g(u))
\end{aligned}$$

So ϕ is a field homomorphism, making ϕ the unique field isomorphism extending θ. □

We proceed to extend Theorem 87 to the case of a splitting field generated by multiple algebraic numbers.

Theorem 88. *******
Let $f(x)\in K[x]$ be a polynomial with no repeated roots and let F be a splitting field for $f(x)$ over K. If $\theta: K\to L$ is a field isomorphism that maps $f(x)$ to $g(x)\in L[x]$ and E is a splitting field for $g(x)$ over L then there exist exactly $[F:K]$ isomorphisms $\phi: F\to E$ such that $\phi(a)=\theta(a)$ for all $a\in K$.

Proof. Let $f(x)\in K[x]$ be a polynomial with no repeated roots and let F be a splitting field for $f(x)$ over K. Let $\theta: K\to L$ be a field isomorphism that maps $f(x)$ to $g(x)\in L[x]$ and E be a splitting field for $g(x)$ over L.
With respect to the diagram we want to prove ϕ is any one of $[F:K]$ isomorphisms.

$$\begin{array}{ccc}
F & \xrightarrow{\phi} & E\\
{\scriptstyle f(x)}\big\downarrow & & \big\downarrow{\scriptstyle g(x)}\\
K & \xrightarrow{\theta} & L
\end{array}$$

We want to show if F is the splitting field of $f(x)$ over K then there exist $[F : K]$ isomorphisms as defined in the statement of the theorem.
We proceed to construct extension fields between F and K and between E and L.
Let $f(x) \in K[x]$ have degree n. Proceeding by induction on the degree of $f(x)$, we assume the result holds for all polynomials of degree less than n and for all fields K.
If $f(x)$ has degree 0 or 1 then $F = K$ and $E = L$ so there is nothing to prove.
Let $p(x)$ be an irreducible factor of $f(x)$ which maps to the irreducible factor $q(x)$ of $g(x)$. Let the degrees of $p(x)$ and $q(x)$ be n.
All the roots of $p(x)$ are elements of F so we may choose one, say u, which gives the tower of fields $K \subseteq K(u) \subseteq F$. Since $f(x)$ has no repeated roots, neither does $p(x)$ and therefore neither does $q(x)$ so we may choose any one, say v, of the d roots of $q(x)$ in E which gives the tower of fields $L \subseteq L(v) \subseteq E$.

$$\begin{array}{ccc} F & \longrightarrow & E \\ | & & | \\ K(u) & \xrightarrow{\psi} & L(v) \\ {\scriptstyle p(x)}\big| & & \big|{\scriptstyle q(x)} \\ K & \xrightarrow{\theta} & L \end{array}$$

By Theorem 81, page 152, the degree d of the minimal polynomial $p(x)$ is equal to $[K(u) : K]$, so the number of roots of $p(x)$ is $d = [K(u) : K]$.
Applying Theorem 87 above there exist $d = [K(u) : K]$ isomorphisms
$\psi : K(u) \to L(v)$ (one for each root v) such that $\psi(u) = v$ and $\psi(a) = \theta(a)$ for all $a \in K$.
Letting $f(x) = (x - u)s(x)$ and $g(x) = (x - v)t(x)$, then the polynomial $s(x)$ has degree less than n, the extension F is a splitting field for $s(x)$ over $K(u)$ and the extension E is a splitting field for $t(x)$ over $L(v)$. Thus the induction assumption may be applied to the setup,

$$\begin{array}{ccc} F & \xrightarrow{\phi} & E \\ {\scriptstyle s(x)}\big| & & \big|{\scriptstyle t(x)} \\ K(u) & \xrightarrow{\psi} & L(v) \\ {\scriptstyle p(x)}\big| & & \big|{\scriptstyle q(x)} \\ K & \xrightarrow{\theta} & L \end{array}$$

and so there exist $[F : K(u)]$ isomorphisms $\phi : F \to E$ such that $\phi(x) = \psi(x)$ for all $x \in K(u)$.
In particular, $\phi(a) = \psi(a) = \theta(a)$ for all $a \in K$.
Therefore we have precisely $[K(u) : K]$ extensions of θ into a ψ and for each ψ we have $[F : K(u)]$ extensions into a ϕ giving, by Theorem 87 above,

$$[F : K(u)][K(u) : K] = [F : K]$$

extensions of the original isomorphism θ. □

Corollary 89. *
Let K be a field with $f(x) \in K[x]$ a polynomial with no repeated roots and let F be a splitting field for $f(x)$ over K. Then $|Gal(F/K)| = [F : K]$

Proof. By definition[2], $|Gal(F/K)|$ is the number of isomorphisms of Theorem 94. □

Before we consider examples of Galois groups let us summarize what we have.

(1) Given an extension field F/K and an element $u \in F$ that is algebraic over K, the degree of the minimal polynomial of u over K is the degree of $K(u)$ as a vector space over K, that is $[K(u) : K]$.

(2) If F is an extension field of K then $[F : K]$ is the degree of the minimal polynomial of an algebraic element in F that is not in K.

(3) Given a finite extension of spitting fields $F/E/K$ then $[F : K] = [F : E][E : K]$

(4) If $f(x) \in K[x]$ is a polynomial of degree $n > 0$ then there exists a splitting field F of $f(x)$ over K with $[F : K] \leq n!$

(5) If F is a splitting field for a separable polynomial $f(x) \in K[x]$ of degree n then $|Gal(F/K)| = [F : K]$ and if $f(x) = a(x - r_1)(x - r_2)\cdots(x - r_n)$ then,

$$|Gal(F/K)| = [F : K] = \prod_{i=1}^{n} deg(p_i(x))$$

is also equal to the product of the degrees of the minimal polynomials $p_i(x)$ of the roots r_i to r_n as we build the tower of fields:

$$\begin{array}{c} F = K(r_i, r_2, \vdots, r_n) \\ | \\ \cdots \\ | \\ K(r_i, r_2) \\ | \\ K(r_i) \\ | \\ K \end{array}$$

[2]Definitions 69, page 161, and 70, page 161.

11.3 Examples of Galois Groups

Example 86. *As an example of both Galois groups, their size, and how they permute the roots of the polynomial, let us consider the base field $K = \mathbb{Q}$ and the splitting field $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ of the polynomial,*

$$f(x) = x^4 - 5x^2 + 6 = (x^2 - 2)(x^2 - 3) = (x + \sqrt{2})(x - \sqrt{2})(x + \sqrt{3})(x - \sqrt{3})$$

First let us note that in building the description of an extension field such as $K(\alpha)$ we define,

$$K(\alpha) = \{a + b\ \alpha \mid a, b \in K\}$$

Accordingly, the extension field $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ and the further extension field is given by,

$$\begin{aligned}\mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}) &= \{x + y\sqrt{3} \mid x, y \in \mathbb{Q}(\sqrt{2})\} \\ &= \{a + b\sqrt{2} + (c + d\sqrt{2})\sqrt{3} \mid a + b\sqrt{2}, c + d\sqrt{2} \in \mathbb{Q}(\sqrt{2}), a, b, c, d \in \mathbb{Q}\} \\ &= \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}\end{aligned}$$

Note that the addition of any two elements of this form still has the structure,

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$$

as does the multiplication of any two elements since that will involve terms like,

$$\sqrt{2} \times \sqrt{3} = \sqrt{6};\ \ \sqrt{2} \times \sqrt{6} = 2\sqrt{3};\ \ \sqrt{3} \times \sqrt{6} = 3\sqrt{2}$$

So a basis for $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ as a vector space over $\mathbb{Q}$ is $\mathfrak{B} = \{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$.
The size of the Galois group is given by $|Gal(F/K)| = [F : K] = |\mathfrak{B}| = 4$.
The four automorphisms in the Galois group are defined by their action on the terms in $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$, specifically by their action on $\sqrt{2}, \sqrt{3}, \sqrt{6}$.
The only[3] *possibilities are,*

$$\begin{aligned}i &: \sqrt{2} \to \sqrt{2}, \sqrt{3} \to \sqrt{3}, \sqrt{6} \to \sqrt{6}, \textit{the identity map fixing all elements} \\ \alpha &: \sqrt{2} \to -\sqrt{2}, \sqrt{3} \to \sqrt{3}, \sqrt{6} \to -\sqrt{6}, \textit{fixing } \sqrt{3} \textit{ only} \\ \beta &: \sqrt{2} \to \sqrt{2}, \sqrt{3} \to -\sqrt{3}, \sqrt{6} \to -\sqrt{6}, \textit{fixing } \sqrt{2} \textit{ only} \\ \gamma &: \sqrt{2} \to -\sqrt{2}, \sqrt{3} \to -\sqrt{3}, \sqrt{6} \to \sqrt{6}, \textit{fixing } \sqrt{6} \textit{ only}\end{aligned}$$

with each map fixing the elements of the base field as required by the definition of $Gal(F/K)$.
The action table where the maps act on the roots and where $a \in \mathbb{Q}$ is,

[3] Why, for instance, is δ fixing $\sqrt{2}$ and $\sqrt{3}$ but not $\sqrt{6}$, that is,

$$\delta : \sqrt{2} \to \sqrt{2}, \sqrt{3} \to \sqrt{3}, \sqrt{6} \to -\sqrt{6}$$

not a member of the Galois group?
The reason is that, since δ is a homomorphism, $\delta(\sqrt{6}) = \delta(\sqrt{2}\sqrt{3}) = \delta(\sqrt{2})\delta(\sqrt{3}) = \sqrt{2}\sqrt{3} = \sqrt{6}$, which is a contradiction to $\delta(\sqrt{6}) = -\sqrt{6}$.

	i	α	β	γ
a	a	a	a	a
$\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$
$\sqrt{3}$	$\sqrt{3}$	$\sqrt{3}$	$-\sqrt{3}$	$-\sqrt{3}$
$\sqrt{6}$	$\sqrt{6}$	$-\sqrt{6}$	$-\sqrt{6}$	$\sqrt{6}$

It is obvious that i, α, β, γ *are permutations of the roots* $\pm\sqrt{2}, \pm\sqrt{3}$ *of*

$$f(x) = x^4 - 5x^2 + 6 = (x^2 - 2)(x^2 - 3) = (x + \sqrt{2})(x - \sqrt{2})(x + \sqrt{3})(x - \sqrt{3})$$

that lie in $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ $\diamond$

Example 87. *Let us continue the previous example for* $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ *over* $K = \mathbb{Q}$. *We identified four automorphisms so that* $|Gal(F/K)| = |Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3})| = 4$. *We can show the size of the Galois group is* $|Gal(F/K)| = 4$ *by another method. We proceed as follows. We built* $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ *in two steps. The minimal polynomial (no roots in* $\mathbb{Q}$*) for the first extension field* $\mathbb{Q}(\sqrt{2})$ *was* $x^2 - 2$ *and for the second extension field* $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ *the minimal polynomial (no roots in* $\mathbb{Q}(\sqrt{2})$ *was* $x^2 - 3$. *The tower of fields is like this,*

$$\begin{array}{r} F = \mathbb{Q}(\sqrt{2}, \sqrt{3}) \\ \Big| \\ p_2(x) = x^2 - 3,\ deg\ 2 \\ \Big| \\ E = \mathbb{Q}(\sqrt{2}) \\ \Big| \\ p_1(x) = x^2 - 2,\ deg\ 2 \\ \Big| \\ K = \mathbb{Q} \end{array}$$

So, by Theorem 87, page 163, using the degrees of the minimal polynomials,

$$[F : E] = 2,\ [E : K] = 2 \Rightarrow [F : K] = 2 \times 2 = 4 = |Gal(F/K)| \qquad \diamond$$

Example 88. *Consider,*

$$\begin{aligned} f(x) &= x^3 - 1 = 0 \\ &\Rightarrow (x - 1)(x^2 + x + 1) = 0 \\ &\Rightarrow x = 1, \omega, \omega^2,\ \omega = -\frac{1}{2} - \frac{\sqrt{3}}{2} \end{aligned}$$

Since the field extension given by,

$$\begin{array}{c} \mathbb{Q}(\omega) \\ | \\ p_1(x) = x^2 + x + 1 \\ | \\ \mathbb{Q} \end{array}$$

is the splitting field of $f(x)$ and the irreducible factor polynomial of $f(x)$ in $\mathbb{Q}$ is x^2+x+1 which has degree 2, then, $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$ so the Galois group of automorphisms acting on the roots of $f(x)$ that fix all roots that are elements of $\mathbb{Q}$, (in this case the root 1), and permute the other roots has just two elements. They can only be the identity automorphism and the automorphism that interchanges ω and ω^2, namely,

$$\begin{aligned} &\phi_0 : \omega \to \omega,\ \omega^2 \to \omega^2,\ \textit{the identity} \\ &\phi_1 : \omega \to \omega^2,\ \omega^2 \to \omega \end{aligned}$$

The Galois group $\{\phi_0, \phi_1\}$ with order 2 is isomorphic to $\mathbb{Z}_2 = \{0, 1\}$ $\diamond$

Let's use a totally different approach to finding a Galois group of a polynomial.

Example 89. *Consider the polynomial $f(x) = x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$. Applying the quadratic formula gives $x^2 = 5 \pm \sqrt{6}$. There is no formula to find the four values of x but by trial and error we can quickly find the four roots,*

$$a = \sqrt{2} + \sqrt{3}, b = \sqrt{2} - \sqrt{3}, c = -\sqrt{2} + \sqrt{3}, d = -\sqrt{2} - \sqrt{3},$$

since each of a^2, b^2, c^2, d^2 is one of $5 \pm 2\sqrt{6}$.
There are $4!$ ways to permute these four roots but not all are members of the Galois group. The members of the Galois group must preserve or fix rational numbers and in particular must preserve any algebraic equation with rational coefficients involving a, b, c, d.
Some of these equations are,

$$ab = -1,\ ac = 1,\ cd = -1,\ bd = 1 \tag{11.3.1}$$

$$a + d = 0,\ b + c = 0 \tag{11.3.2}$$

Of course we chose the equations that produce rational numbers so that we can form equations such as,

$$ab = -1 \Rightarrow \phi(ab) = \phi(-1) \Rightarrow \phi(a)\phi(b) = -1 \Rightarrow \phi(b) = \frac{-1}{\phi(a)} \tag{11.3.3}$$

Note we use the definition that ϕ is an automorphism that fixes rationals, so $\phi(-1) = -1$.
In a similar fashion we can form the equations,

$$\phi(c) = \frac{1}{\phi(a)};\ \phi(d) = -\phi(a) \tag{11.3.4}$$

It then follows that the only permutations that obey these relationships are the identity and three others, namely,

$$\begin{aligned}\phi_0 &: (a,b,c,d) \to (a,b,c,d)\\ \phi_1 &: (a,b,c,d) \to (b,a,d,c)\\ \phi_2 &: (a,b,c,d) \to (c,d,a,b)\\ \phi_3 &: (a,b,c,d) \to (d,c,b,a)\end{aligned}$$

Let's consider any one of these, say ϕ_2. Its action upon (a,b,c,d) is,

$$\phi_2(a) = c,\ \phi_2(c) = a,\ \phi_2(b) = d,\ \phi_2(d) = b$$

Now, applying the equation $\phi_2(c) = \dfrac{1}{\phi(a)}$ to the pair $\phi_2(a) = c,\ \phi_2(c) = a$, we have $ac = \phi_2(c)\phi_2(a) = \dfrac{1}{\phi(a)}\phi(a) = 1$ and similarly $bd = 1$. In other words, the required relationships of (11.3.1) hold for $\phi(2)$ so it is a member of the Galois group, and you can easily show this is also true for ϕ_1, ϕ_3, ϕ_4.
But if we try any other permutation we find these relationships do not hold (so it is not a member of the Galois group).
For example, let's suppose $\phi : (a,b,c,d) \to (b,c,a,d)$ is a member of the Galois group. Then, $\phi(a) = b,\ \phi(b) = c$.
But by (11.3.4) above, $\phi(b) = -\dfrac{1}{\phi(a)} \Rightarrow c = -\dfrac{1}{b}$. But then $b + c = b - \dfrac{1}{b} = \dfrac{b-1}{b} \neq 0$ since $b = \sqrt{2} - \sqrt{3}$.
So we have a contradiction to (11.3.2) above which states $b + c = 0$. ⋄

Example 90. *Consider $f(x) = x^3 - 2$ over $\mathbb{Q}$?*
We have[4]*,*

$$\begin{aligned}&x^3 - 2 = 0\\ &\Rightarrow x^3 = 2\\ &\Rightarrow x = \sqrt[3]{2}\ e^{\frac{2\pi i k}{3}},\ k = 0,1,2\\ &\Rightarrow x = \sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2,\ \omega = \frac{-1+\sqrt{3}i}{2}\end{aligned}$$

Note ω is a root of the irreducible monic polynomial $x^2 + x + 1$, so the splitting field for $f(x)$ over $\mathbb{Q}$ is therefore $F = \mathbb{Q}(\sqrt[3]{2}, \omega)$. The tower of fields with monic polynomials indicated is,

[4]Please refer to Section 1.4 where we first encountered cube roots and the 3rd roots of unity

$$\begin{array}{r} \mathbb{Q}(\sqrt[3]{2},\omega) \\ \Big| \\ p_2(x) = x^2 + x + 1,\ deg\ 2 \\ \Big| \\ \mathbb{Q}(\sqrt[3]{2}) \\ \Big| \\ p_1(x) = x^3 - 2,\ deg\ 3 \\ \Big| \\ \mathbb{Q} \end{array}$$

The three zeros of $x^3 - 2$ *are* $\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$. *The two zeros of* $x^2 + x + 1$ *are* ω, ω^2. *We proved in Theorem 92, page 177, that the automorphisms permute the roots, so if* $\phi \in Gal(F/\mathbb{Q})$ *then,*

$$\begin{aligned} \phi(\sqrt[3]{2}) &= \sqrt[3]{2}\ or\ \sqrt[3]{2}\omega\ or\ \sqrt[3]{2}\omega^2 \\ \phi(\omega) &= \omega\ or\ \omega^2 \end{aligned}$$

So we have six automorphisms[5]*, namely,*

$$\begin{aligned} \phi_0 &: \sqrt[3]{2} \to \sqrt[3]{2},\ \omega \to \omega \\ \phi_1 &: \sqrt[3]{2} \to \sqrt[3]{2},\ \omega \to \omega^2 \\ \phi_2 &: \sqrt[3]{2} \to \sqrt[3]{2}\omega,\ \omega \to \omega \\ \phi_3 &: \sqrt[3]{2} \to \sqrt[3]{2}\omega,\ \omega \to \omega^2 \\ \phi_4 &: \sqrt[3]{2} \to \sqrt[3]{2}\omega^2,\ \omega \to \omega \\ \phi_5 &: \sqrt[3]{2} \to \sqrt[3]{2}\omega^2,\ \omega \to \omega^2 \end{aligned}$$

Then the Galois group has six elements or is of order 6. It is isomorphic to a finite group of order 6. There are two possibilities, the abelian group $\mathbb{Z}_6$ *and the non-abelian symmetric group* S_3. *Note, however, that,*

$$\begin{aligned} \phi_2 \circ \phi_1(\sqrt[3]{2}) &= \phi_2(\sqrt[3]{2}) = \sqrt[3]{2}\omega \\ but\ \phi_1 \circ \phi_2(\sqrt[3]{2}) &= \phi_2(\sqrt[3]{2}\omega) = \phi_2(\sqrt[3]{2})\phi_2(\omega) = \sqrt[3]{2}\omega \cdot \omega \end{aligned}$$

so the Galois group is not abelian and therefore $Gal(\mathbb{Q}(\sqrt[3]{2}\omega)/\mathbb{Q}) \cong S_3$. ◇

11.4 Multiple Roots

Next, we need to discuss the possibility that $f(x)$ has some roots that are the same. We will find that we always need the roots to be simple, that is $f(x)$ has no multiple roots.

[5]Note also the product of the degrees of the minimal polynomials in the tower is also 6.

Definition 71. *multiple roots*
If $f(x)$ has the factorization,

$$f(x) = (x - r_1)^{m_1} \cdots (x - r_s)^{m_s}),$$

we say the root r_i has multiplicity m_i.

Definition 72. *simple roots*
If $m_i = 1$ we say r_i is a simple root.

To determine whether a polynomial has multiple roots, we prove in Theorem 90 that $f(x) \in K[x]$ has no multiple roots if and only if $gcd(f(x), f'(x)) = 1$. Since our base field is $\mathbb{Q}$, the symbol $f'(x)$ is the ordinary derivative[6] of $f(x)$ in $\mathbb{Q}$.

Theorem 90. *** A non-constant polynomial $f(x)$ over the field $\mathbb{R}$ of real numbers has no repeated roots if and only if $gcd(f(x), f'(x)) = 1$, where $f'(x)$ is the usual derivative of $f(x)$ with respect to x.*

Proof. We need to prove two implications,

(a) $f(x)$ has no repeated roots implies $gcd(f(x), f'(x)) = 1$.

(b) $gcd(f(x), f'(x)) = 1$ implies $f(x)$ has no repeated roots

In both cases we will prove the contrapositives,

(a) $gcd(f(x), f'(x)) \neq 1$ implies $f(x)$ has repeated roots.

(b) $f(x)$ has repeated roots implies $gcd(f(x), f'(x)) \neq 1$.

First, suppose $gcd(f(x), f'(x)) = d(x) \neq 1$. Then let $p(x)$ be an irreducible factor of $d(x)$. Then,

$$f(x) = p(x)a(x) \text{ and } f'(x) = p(x)b(x) \tag{11.4.1}$$

for some $a(x), b(x) \in \mathbb{R}[x]$.
By the product rule of differentiation we also have,

$$\begin{aligned} f'(x) &= a'(x)p(x) + a(x)p'(x) \\ \Rightarrow p(x)b(x) &= a'(x)p(x) + a(x)p'(x) \text{ by (11.4.1)} \\ \Rightarrow a(x)p'(x) &= p(x)[a'(x) - b(x)] \end{aligned}$$

Since $p(x) \nmid p'(x)$ this means $p(x) | a(x)$, say $a(x) = c(x)p(x)$ for some $c(x) \in \mathbb{R}[x]$. Then $f(x) = a(x)p(x) = c(x)p^2(x)$ and $f(x)$ has a repeating factor, thus proving $f(x)$ has no repeated roots implies $gcd(f(x), f'(x)) = 1$.

[6] Again, if you have not studied Calculus, you can simply accept we have a process for determining whether a polynomial has multiple roots. Theorem 72B, page 129 is another proof of this theorem.

*****

Conversely, suppose $f(x)$ has a repeated factor, say $f(x) = g^n(x)q(x),\ n > 1$. Then,

$$\begin{aligned} f'(x) &= ng^{n-1}(x)g'(x)q(x) + g^n q'(x) \\ &= g(x)[ng^{n-2}(x)g'(x)q(x) + g^{n-1}(x)q'(x)] \end{aligned}$$

which means $g(x)$ also divides $f'(x)$ and so the $gcd(f(x), f'(x)) \geq g(x) \neq 1$. This proves that $f(x)$ has repeated roots implies $gcd(f(x), f'(x)) \neq 1$. □

11.5 Separable Polynomials

We will find, in our pursuit of unsolvable polynomials that we want our polynomials to have no multiple roots. We define,

Definition 73. *separable polynomial*
We define a polynomial as separable if its irreducible factors have only simple roots, that is, no multiple roots.

Definition 74. *separable field*
Given an algebraic extension field F over K as a field in which all the elements are algebraic over K, that is, every element in F is the root of a nonzero polynomial $f(x) \in K$, we say F is a separable field if the minimal polynomial of each element of F is separable, that is if each of its irreducible factors does not have multiple roots.

Example 91. *For example, $f(x) = x^4 - 5x^2 + 6 = (x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x]$ has an algebraic extension field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ which is separable since the minimal polynomials $x^2 - 2$ and $x^2 - 3$ have the irreducible factors $(x + \sqrt{2}), (x - \sqrt{2}), (x + \sqrt{3})$ and $(x - \sqrt{3})$, that is $f(x)$ has the simple roots $\pm\sqrt{2}, \pm\sqrt{3}$.* ◇

Finally, we prove in the difficult Theorem 91 that if F is separable over K then it is a simple extension of K, that is $F = K(\gamma)$ for some $\gamma \in F$.

Theorem 91. *****
Let F be a finite, separable extension of a field K. Then $F = K(\gamma)$ for some $\gamma \in F$.

Proof. We proceed by induction. We first prove the result in the case $F = K(\alpha_1, \beta_1)$. For our purposes $K = \mathbb{Q}$ which is an infinite field so we suppose K is an infinite field.
Let $F = K(\alpha_1, \beta_1), \alpha_1, \beta_1 \in F$. We want to show $F = K(\gamma),\ \gamma \in F$.
Let $f(x), g(x)$ be the minimal polynomials of α_1, β_1, so that $f(\alpha_1) = 0,\ g(\beta_1) = 0$ and assume the minimal polynomials have degree m, n respectively.
Let E be an extension of F over which both $f(x), g(x)$ split.
Since F is separable, the roots $\alpha_1, \alpha_2, \ldots, \alpha_m$ and $\beta_1, \beta_2, \ldots, \beta_n$ of $f(x)$ and $g(x)$ are distinct and all lie in E.
If $j \neq 1$, the equation $\alpha_i + \beta_j x = \alpha_1 + \beta_1 x$ has a unique solution $x = \dfrac{\alpha_i - \alpha_1}{\beta_1 - \beta_j}$ in E.

But there are only a finite number of such an x since there are only a finite number of α_i given $i = 2, 3, \ldots, m$, and only a finite number of β_j given $j = 2, 3, \ldots, n$.
So since K and therefore E have an infinite number of elements there must be (an infinite number of) elements a such that $a \neq \dfrac{\alpha_i - \alpha_1}{\beta_1 - \beta_j}$ or $\alpha_1 + a\beta_1 \neq \alpha_i + a\beta_j$ for $\alpha_i \neq \alpha_1$ and $\beta_j \neq \beta_1$.
Then, for one such value of a let $\gamma = \alpha_1 + a\beta_1$. We shall prove $F = K(\alpha_1, \beta_1) = K(\gamma)$.
It is clear that $K(\gamma) = K(\alpha_1 + a\beta_1) \subseteq F = K(\alpha_1, \beta_1)$ since if $a, \alpha_1, \beta_1 \in F$ then so does $\alpha_1 + a\beta_1$.
Now if we can show $\beta_1 \in K(\gamma)$ then so does $-a\beta_1$ and then,

$$-a\beta_1 \in K(\gamma) \text{ and } \gamma = \alpha_1 + a\beta_1 \in K(\gamma) \Rightarrow \alpha_1 + a\beta_1 - a\beta_1 \Rightarrow \alpha_1 \in K(\gamma)$$

We could then conclude $\alpha_1 + a\beta_1 \in K(\gamma)$ so that $K(\alpha_1, \beta_1) \subseteq K(\gamma)$ and double containment gives the equality $K(\alpha_1, \beta_1) = K(\gamma)$.

******

So let's prove $\beta_1 \in K(\gamma)$.
Now, in general, if the minimal polynomial of an algebraic number u over a field K has degree 1, (of the form $x - u$), then u must be an element of K.
Our strategy therefore is to prove the minimal polynomial $p(x)$ of β_1 over $K(\gamma)$ is linear or has degree 1 (of the form $(x - \beta_1)$) so that $\beta_1 \in K(\gamma)$.
Let $h(x) = f(\gamma - ax)$, where $\gamma = \alpha_1 + a\beta_1$. This polynomial has coefficients $-a$ and γ in $K(\gamma)$ and,

$$h(\beta_1) = f(\gamma - a\beta_1) = f(\alpha_1) = 0,$$

since $f(x)$ is the minimal polynomial of α_1 over K. Thus β_1 is a root of $h(x)$ as well as of its own minimal polynomial $g(x)$.
We note, by Theorem 78, page 145, the minimal polynomial $p(x)$ of β_1 over $K(\gamma)$ must divide both $h(x)$ and $g(x)$.
We consider all three polynomials, $p(x), g(x), h(x)$ over the extension field E.
Since $\gamma = \alpha_1 + a\beta_1$ and $\alpha_1 + a\beta_1 \neq \alpha_i + a\beta_j$ then $\gamma \neq \alpha_i + a\beta_j$ so $\gamma - a\beta_j \neq \alpha_i$ for $1 \leq i \leq m$ and $2 \leq j \leq n$. This means,

$$h(\beta_j) = f(\gamma - a\beta_j) \neq f(\alpha_i) = 0,$$

so β_j is not a root of $h(x)$ for $2 \leq j \leq n$.
Therefore since $g(x) = b(x - \beta_1)(x - \beta_2)\cdots(x - \beta_n)$ only β_1 is a root of both $g(x)$ and $h(x)$.
We can conclude that over E, the $gcd(h(x), g(x)) = x - \beta_1$. But the minimal polynomial $p(x)$ is a common divisor of $h(x)$ and $g(x)$ over E as well as over $K(\gamma)$, so we must have $p(x) = x - \beta_1$ or it is linear.
We have therefore proved in the case $F = K(\alpha_1, \beta_1)$ that $F = K(\gamma), \gamma = \alpha_1 + a\beta_1$. We proceed to prove the general result by induction.

*****

Reformatting this result, we have proved $F = K(\alpha_1, \alpha_2) \Rightarrow F = K(\gamma_2)$ say.
Suppose $F = K(\gamma_{n-1})$ is true for $F = K(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})$.
We want to prove the result is true for $F = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$, that is, $F = K(\gamma_n)$.
Now,

$$\begin{aligned} F &= K(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, \alpha_n) \\ &= K(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})(\alpha_n) \\ &= K(\gamma_{n-1})(\alpha_n) \text{ by the assumption} \\ &= K(\gamma_{n-1}, \alpha_n) \end{aligned}$$

But this is just the case $F = K(\alpha_1, \beta_1)$, so we are done, concluding $F = K(\gamma_n)$ for some $\gamma_n \in F$. □

Chapter 12

Fundamental Theorem of Galois Theory

The fundamental theorem of Galois Theory determines a one-to-one correspondence for the extension field F/K of the intermediate fields between F and K with the subgroups of the Galois group $Gal(F/K)$. The tower or lattice of these intermediate fields corresponds to the inverted tower or lattice of the subgroups of the Galois group.

12.1 The G-fixed subfield of a field F

Note 23. *First let us recall the test for a subfield. We say a subset K of a field F is a subfield if and only if K is a field under the same addition and multiplication operations that apply to F. That is, K is a subgroup of F under addition and the nonzero elements $K^\times$ of K are a subgroup of F under multiplication. The subfield test therefore is that for subgroups under the two operations of addition and multiplication. Accordingly, $K \subseteq F$ is a subfield of F if and only if,*

- *If $a, b \in K$ then $a - b \in K$.*
- *If $a, b \in K^\times$ then $ab^{-1} \in K^\times$.*

We first prove in Theorem 92 that for a field F and a subgroup G of $Aut(F)$ that the set,

$$\{a \in F \mid \phi(a) = a \text{ for all } \phi \in G\}$$

is a subfield of F, that is the elements in F that are fixed by all the automorphisms in the subgroup G form a subfield of F.

Theorem 92. *****
Let F be a field and G a subgroup of $Aut(F)$.
Then $E = \{a \in F \mid \phi(a) = a \text{ for all } \phi \in G\}$ is a subfield of F.

Proof. Let F be a field and $G < Aut(F)$.
To show $E = \{a \in F \mid \phi(a) = a \text{ for all } \phi \in G\}$ is a field, we need to show it is a subgroup under both operations. We use the subfield tests outlined in Note 25 on page 183.
Let $a, b \in E$. Let $\phi \in G$. We need to show $a - b \in E$ and $ab^{-1} \in E$. The argument is the same for both operations.
First, if $b \in E$, then $b^{-1} \in E$, since $\phi(b^{-1}) = \phi(b)^{-1} = b^{-1}$ so ϕ fixes b^{-1}.
But then for all $\phi \in G$, $\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = ab^{-1}$, so that ϕ fixes ab^{-1} making $ab^{-1} \in E$.
Thus E is a subfield of F. □

We now change the notation from E to one more informative.

Definition 75. *G-fixed subfield of a field*
The elements in a field F that are fixed by all the automorphisms in the subgroup G of $Aut(F)$ are called the G–fixed subfield of F and we denote it by F^G, that is,

$$F^G = \{a \in F \mid \phi(a) = a \text{ for all } \phi \in G\}$$

Example 92. *Let's extend our example for $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, where $Gal(F/\mathbb{Q}) = \{i, \alpha, \beta, \gamma\}$, with these elements given by,*

$$\begin{aligned}
i &: \sqrt{2} \to \sqrt{2}, \sqrt{3} \to \sqrt{3}, \sqrt{6} \to \sqrt{6}, \textit{the identity map fixing all elements} \\
\alpha &: \sqrt{2} \to -\sqrt{2}, \sqrt{3} \to \sqrt{3}, \sqrt{6} \to -\sqrt{6}, \textit{fixing } \sqrt{3} \textit{ only} \\
\beta &: \sqrt{2} \to \sqrt{2}, \sqrt{3} \to -\sqrt{3}, \sqrt{6} \to -\sqrt{6}, \textit{fixing } \sqrt{2} \textit{ only} \\
\gamma &: \sqrt{2} \to -\sqrt{2}, \sqrt{3} \to -\sqrt{3}, \sqrt{6} \to \sqrt{6}, \textit{fixing } \sqrt{6} \textit{ only}
\end{aligned}$$

The subgroup $G = \{i, \alpha\}$ consists of the identity automorphism i which fixes every element of F and α which fixes every element of $\mathbb{Q}$ as well as $\sqrt{3}$ and replaces $\sqrt{2}, \sqrt{6}$ with their additive inverses.
So the functions in $G = \{i, \alpha\}$ cause a permutation of the roots $\{\pm\sqrt{2}, \pm\sqrt{3}\}$ by exchanging $\sqrt{2}$ with $-\sqrt{2}$ but leave $\pm\sqrt{3}$ fixed along with all rational numbers.
Accordingly, $F^G = F^{\{i,\alpha\}} = \{\sqrt{3}, a \mid a \in \mathbb{Q}\}$. ◇

We next prove in Theorem 93 that if F is the splitting field over K of a separable polynomial and $G = Gal(F/K)$, then, $F^G = F^{Gal(F/K)} = K$.

Theorem 93. *****
If F is the splitting field over K of a separable polynomial $f(x)$, then $F^{Gal(F/K)} = K$.

Proof. Say $f(x) = a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_r)$. With $G = Gal(F/K)$ we have the tower of fields,

$$\begin{array}{c} F = K(\alpha_1, \alpha_2, \ldots, \alpha_r) \\ | \\ F^G = \{a \in F \mid \phi(a) = a \text{ for all } \phi \in G\} \\ | \\ K \end{array}$$

F^G does not contain any of the α_i since by Theorem 86, page 162, the automorphisms ϕ permute all the roots of $f(x)$ which is not the case for F^G. So F is a splitting field over F^G as well as over K. Thus the automorphisms of $Gal(F/F^G)$ are the same as those of $Gal(F/K)$ making $Gal(F/F^G) = Gal(F/K)$.
By Corollary 89, page 166, we have both,

$$|Gal(F/K)| = [F : K] \text{ and } |Gal(F/F^G)| = |Gal(F/K)| = [F : F^G]. \tag{12.1.1}$$

By Theorem 83, page 154, $[F : K] = [F : F^G] \cdot [F^G : K]$, so substituting (12.1.1) we have,

$$|Gal(F/K) = |Gal(F/K)| \cdot [F^G : K]$$

Hence, $[F^G : K] = 1$.
This means a basis for F^G over K has just the one element, the identity element e. Hence every element of F^G is just e times an element of K which means $F^G = K$. □

Example 93. *In our above example, $K = \mathbb{Q}$ and $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, so F is the splitting field of,*

$$f(x) = x^4 - 5x^2 + 6 = (x - \sqrt{2})(x + \sqrt{2})(x + \sqrt{3})(x - \sqrt{3})$$

and $G = Gal(F/\mathbb{Q}) = \{i, \alpha, \beta, \gamma\}$. Then only the elements of $\mathbb{Q}$ are fixed by all of i, α, β, γ so that $F^G = \mathbb{Q}$. ◇

Artin proved in Theorem 94 that if G is a finite group of automorphisms of a field F then the degree of F as a vector space over F^G is less than or equal to the number of elements in G, that is, $[F : F^G] \leq |G|$.

Note 24. *Let us first review some facts from the theory of systems of linear equations. A system of n linear equations in $n+1$ variables all equal to zero has an infinite number of solutions since if we select one of the variables we can express all the other variables in terms of it, so this selected variable can be given any value at all. For example, consider,*

$$2x + y + z = 0 \tag{12.1.2}$$

$$6x - y + 3z = 0 \tag{12.1.3}$$

Then (12.1.2)+(12.1.3) gives $8x + 0y + 4z = 0 \Rightarrow z = -2x$.
Substituting in (12.1.2) we obtain $y = 0$.

Hence the infinite number of solutions of the three equations are $(x, 0, -2x)$ *for any* $x \in \mathbb{R}$, *for example* $(1, 0, -2)$ *and* $(-2, 0, 4)$.
Clearly we can then multiply or divide any solution by a constant a to get $(ax, 0, -2ax)$ *which is another solution since (substituting into (12.1.2))* $2ax + 0 - 2ax = 0$.
And we can add solutions together to get further solutions, for example,

$$(1, 0, -2) + (-2, 0, 4) = (-1, 0, 2)$$

Theorem 94. ***** (Artin)*
Let F *be a field and* G *a subgroup of* $Aut(F)$. *Then* $[F : F^G] \leq |G|$.

Proof. Let $G = \{\phi_1 = id, \phi_2, \ldots, \phi_n)$ where each $\phi_i \in Aut(F)$.
We may regard F as a vector space over F^G with dimension $[F : F^G]$.
Recall Definition 61, page 149, that a set of vectors $\{a_1, a_2, \ldots, a_{n+1}\}$ in a vector space over a field F is linearly independent only if any linear combination of them is never trivially zero, that is if the $b_i \in F$ are scalars then,

$$a_1b_1 + a_2b_2 + \ldots + a_{n+1}b_{n+1} \neq 0$$

unless all the b_i are 0.
So suppose there exist $(n + 1)$ elements $\{a_1, a_2, \ldots a_{n+1}\}$ of F that are linearly independent over F^G. We will prove this supposition is false.
Consider the system of equations,

$$\begin{aligned}
\phi_1(a_1)x_1 + \phi_1(a_2)x_2 + \ldots + \phi_1(a_{n+1})x_{n+1} &= 0 \\
\phi_2(a_1)x_1 + \phi_2(a_2)x_2 + \ldots + \phi_2(a_{n+1})x_{n+1} &= 0 \\
&\ldots \\
\phi_n(a_1)x_1 + \phi_n(a_2)x_2 + \ldots + \phi_n(a_{n+1})x_{n+1} &= 0
\end{aligned}$$

The system has n equations and $n+1$ unknowns so there exists at least one non-trivial solution, say $(b_1, b_2, \ldots, b_{n+1})$ in F. We choose the solution with the smallest number of non-zero elements and rearrange its elements if necessary so that $b_1 \neq 0$. Dividing each b_i by b_1 gives another solution $\left(1, \frac{b_2}{b_1} \ldots, \frac{b_{n+1}}{b_1}\right)$ which we may again call simply,

$$(1, b_2, \ldots, b_{n+1}). \tag{12.1.4}$$

Since $\phi_1 = identity$ or $\phi_1(a_i) = a_i$ for all $(a_1, a_2, \ldots, a_{n+1})$, we have for the first equation in the system,

$$\begin{aligned}
\phi_1(a_1)x_1 + \phi_1(a_2)x_2 + \ldots + \phi_1(a_{n+1})x_{n+1} &= 0 \\
\Rightarrow a_1x_1 + a_2x_2 + \ldots + a_{n+1}x_{n+1} &= 0
\end{aligned}$$

Now, not all of the elements b_i from (12.1.4) can belong to F^G since, substituting, we have $a_1b_1 + a_2b_2 + \ldots + a_{n+1}b_{n+1} = 0$ which would contradict the assumption that

the elements $\{a_1, a_2, \ldots, a_{n+1}\}$ are linearly independent over F^G, since all the b_i and specifically $b_1 = 1$ are not zero.
We now rearrange the elements so that, say, $b_2 \notin F^G$.
Since $F^G = \{c \in F \mid \phi(c) = c \text{ for all } \phi \in G\}$ and $b_2 \notin F^G$, this means b_2 is not fixed by all the automorphisms in G. Let's say $\phi_k(b_2) \neq b_2$.
If we apply ϕ_k to each of the elements, $(b_1, b_2, \ldots, b_{n+1})$, we do not change the elements since multiplying each element by ϕ_k merely permutes the system.
However, noting $\phi_k(1) = 1$, we do get a second solution,

$$(1, \phi_k(b_2), \ldots, \phi_k(b_{n+1})) \tag{12.1.5}$$

Subtracting this second solution 12.1.5 from the first solution 12.1.4 gives a non-trivial third solution,

$$(0, \phi_k(b_2) - b_2, \ldots, \phi_k(b_{n+1}) - b_{n+1}), \tag{12.1.6}$$

which is non-trivial since at least $\phi_k(b_2) - b_2 \neq 0$.
But this third solution has at least one fewer[1] non-zero terms than (12.1.4), contradicting the assumption that we chose the solution with the smallest number of non-zero elements. Hence there do not exist $n+1$ elements $\{a_1, a_2, \ldots, a_{n+1}\}$ of F that are linearly independent over K.
So a basis for F over F^G has less than $n+1$ elements.
Accordingly, $[F : F^G] \leq n = |G|$. □

Recall we defined in Definition 57 on page 146 that if $u \in F$ is algebraic over K then the monic polynomial $p(x)$ of minimal degree in $K[x]$ such that $p(u) = 0$ is called the minimal polynomial of u over K.
Recall also Definition 67 on page 157 that an extension field F of K is called a splitting field for

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

over K if there exist elements $r_1, r_2, \ldots, r_n$ such that,

- $f(x) = a_n(x - r_1)(x - r_2)\cdots(x - r_n)$
- $F = K(r_1, r_2, \ldots, r_n)$

Definition 76. *normal extension*
indexnormal extension If F is an algebraic extension of a field K then F is said to be a normal extension of K if every irreducible polynomial in $K[x]$ that contains a root in F is a product of linear factors in $F[x]$.

[1] Since the leading term has been changed from a "1" to a "0".

Example 94. *For example,* $\mathbb{Q}(\sqrt{2})$ *is a normal extension of* $\mathbb{Q}$ *since it is the splitting field of* $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$.
But $\mathbb{Q}(\sqrt[3]{2})$ *is not a normal extension of* $\mathbb{Q}$ *since the minimal polynomial is*

$$x^3 - 2 = (x - \sqrt[3]{2})(x - \omega\sqrt[3]{2})(x - \omega^2\sqrt[3]{2}),\ \omega = \frac{-1 + \sqrt{3}}{2}$$

and $\mathbb{Q}(\sqrt[3]{2})$ *does not contain* ω. ◇

Theorem 95. ******
Let F *be an extension field of* K. *The following statements are equivalent.*

(1) F *is the splitting field*[2] *over* K *of a separable*[3] *polynomial.*

(2) $K = F^G$ *for some finite group* G *of automorphisms of* F.

(3) F *is a finite, normal*[4]*, separable*[5] *extension*[6] *of* K.

Proof. Let F be an extension field of K. We have three parts to prove.

(1) ⇒ (2)
We need to show if F is the splitting field over K of a separable polynomial then $K = F^G$ for some finite group G of automorphisms of F,
First we need to find a group G such that $K = F^G$. But in Theorem 93, page 177, we proved if F is the splitting field over K of a separable polynomial $f(x) \in K[x]$, then $F^{Gal(F/K)} = K$, so for G we have $Gal(F/K)$.
Second we need to show our G is finite. But by Corollary 89, page 166, we have $|Gal(F/K)| = [F : K]$, and since by Theorem 84, page 158, $[F : K] \leq n!$ where n is the degree of $f(x)$ and is therefore finite, then G has a finite number of elements.

*****

(2) ⇒ (3).
We need to show if $K = F^G$ for some finite group G of automorphisms of F, then,

(a) F is a finite extension of K. This is clear since F is the splitting field over K of a separable polynomial which can only have as many roots and therefore extensions of K as its finite degree.

(b) F is a separable extension of K, which will be the case if the minimal polynomial of each element of F is separable, that is, does not have multiple roots.
So let $p(x) \in K[x]$ be any irreducible polynomial in K and $\alpha \in F$ be a zero of

[2]Definition 67, page 157
[3]Definition 73, page 173
[4]Definition 76, page 180
[5]Definition 74, page 173
[6]Definition 55, page 142

$p(x)$.
Let the number of distinct elements in the set $\{\phi(\alpha) \mid \phi \in G\}$ be n. Then these elements are the results of the $\phi's$ acting on α which we will label $\alpha_1, \alpha_2, \ldots, \alpha_n$. One of the $\phi's$ is the identity so let's say $\alpha_1 = \alpha$.
Consider the polynomial,

$$h(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n) \tag{12.1.7}$$
$$= x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0, \text{ say.} \tag{12.1.8}$$

If $\alpha_1 = \alpha$, then $h(\alpha_1) = h(\alpha) = 0$. Applying any of the $\phi's$ to (12.1.7) and (12.1.8) we have,

$$(x-\phi(\alpha_1))(x-\phi(\alpha_2))\cdots(x-\phi(\alpha_n)) \tag{12.1.9}$$
$$= x^n + \phi(a_{n-1})x^{n-1} + \ldots + \phi(a_1)x + \phi(a_0) \tag{12.1.10}$$

But since by Theorem 86, page 162, ϕ simply permutes the α_i, the product of the $(x-a_i)$ in (12.1.7) and the $(x-\phi(a_i))$ in (12.1.9) are the same, from which we conclude from (12.1.8) and (12.1.10) that,

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$$
$$= x^n + \phi(a_{n-1})x^{n-1} + \ldots + \phi(a_1)x + \phi(a_0)$$

So $\phi(a_i) = a_i$ for all i, and therefore the coefficients a_i of $h(x)$ all belong to,

$$F^G = \{a \in F \mid \phi(a) = a \text{ for all } \phi \in G\}$$

Since $K = F^G$ and $h(x) \in K[x]$ and $h(\alpha) = 0$, and since $p(x) \in K[x]$ and is irreducible and, by definition of the minimal polynomial, $p(\alpha) = 0$, then we must have $p(x)|h(x)$ in $K[x]$ by Theorem 78 on page 145.
It follows that $p(x)$ is the product of some of the $(x-a_i)$. Since all of these are distinct, $p(x)$ is separable and has all of its zeros in F. Then since $p(x)$ is any irreducible polynomial in $K[x]$, F is a separable extension of K.

(c) F is a normal extension of K, meaning every irreducible polynomial in $K[x]$ that has a root in F is the product of linear factors in F.
This is true since any polynomial in $K[x]$ with a root in F factors into irreducible polynomials in $K[x]$ and, by what we have proved, each of these is separable and has only linear factors in F, then we have a normal[7] extension.

*****

(3) $\Rightarrow$ (1).
We need to show if F is a finite, normal, separable extension of K, that is, every irreducible polynomial in $K[x]$ that has a root in F is a product of linear factors in

[7]Definition 74, page 173

F, then F is the splitting field over K of a separable polynomial,
By Theorem 91, page 173, F is a simple extension, say $F = K(\gamma)$. If F is a normal extension of K and γ has a minimal polynomial $f(x) \in K[x]$, then by Definition 76, page 180, F contains all the roots of $f(x)$ making it a splitting field for $f(x)$. □

Definition 84. *Galois extension*
We define a finite extension field F of a field K to be a Galois extension if it satisfies any and hence all of the conditions in Theorem 101. Thus a Galois extension may also be called a normal extension.

Note 25. *There are two ways for an extension not to be a Galois extension. One is for it to not be a normal extension, which if it contains one root of a polynomial, must contain all the roots. For instance, $\mathbb{Q}(\sqrt[4]{2})$ is not normal, and hence not Galois, since it is missing the complex roots $\pm\sqrt[4]{2}e^{2\pi i\frac{k}{4}}$, $k = 1, 2, 3$, of $x^4 - 2$, and therefore is not a splitting field for $f(x) = x^4 - 2$.*
Another possibility for a non-Galois extension is for it to be not separable. But for us, all polynomials $f(x) \in \mathbb{Q}[x]$ are separable into distinct linear factors.

Corollary 96 is that if F is an extension field of K and,

$$K = F^G = \{a \in F \mid \phi(a) = a \text{ for all } \phi \in G, G < Aut(F)\}$$

then $G = Gal(F/K)$.

Corollary 96. *****
If F is an extension field of K such that $K = F^G$ for some finite group G of automorphisms of F then $G = Gal(F/K)$.

Proof. Given

$$K = F^G = \{a \in F \mid \phi(a) = a \text{ for all } \phi \in G\}$$
$$Gal(F/G) = \{\phi \in AutF \mid \phi(a) = a \text{ for all } a \in G\},$$

then G is a subgroup of $Gal(F/K)$, so we have $|G| \le |Gal(F/K)|$.
By Theorem 95 above if $K = F^G$ for some finite group G of automorphisms of F then equivalently F is the splitting field over K of some separable polynomial.
Since this is the condition required by Corollary 89, page 166, we have
$|Gal(F/K)| = [F : K]$.
But by Artin's Lemma, Theorem 94, page 179, we have $[F : K] \le |G|$, so we conclude $|Gal(F/K)| \le |G|$.
Together with the earlier statement $|G| \le |Gal(F/K)|$, this means

$$G = Gal(F/K).$$

□

12.2 The Fundamental Theorem of Galois Theory

We are almost ready to prove the fundamental theorem. It requires a group theory proof, Theorem 97, which we prove upfront. It states:

Theorem 97. *Let $\phi : G \to H$ be a group homomorphism between groups G, H. Let $e \in H$ be the identity element. Then the kernel of ϕ is a normal subgroup of G.*

Proof. Let $\phi : G \to H$ be a group homomorphism between groups G, H. Let $e_1 \in G, e_2 \in H$ be the identity elements.
Recall the kernel of a group homomorphism ϕ acting on a group G is defined in Definition 26 on page 55 by $ker(\phi) = \{g \in G \mid \phi(g) = e_2\}$ where e_2 is the identity element in H.
Let $k \in ker(\phi)$ so that $\phi(k) = e_2$.
Then, by Definition 31, page 65, $ker(\phi)$ is a normal subgroup of G if $gkg^{-1} \in ker(\phi)$ for all $g \in G$ and $k \in ker(\phi)$, that is, $\phi(gkg^{-1}) = e_2$. But,

$$\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g^{-1}) = \phi(g)e_2\phi(g^{-1}) = \phi(gg^{-1}) = \phi(e_1) = e_2$$

Hence, $gkg^{-1} \in ker(\phi)$ so that the kernel of ϕ is a normal subgroup of G. □

Theorem 98. ****** Fundamental Theorem of Galois Theory*
Let F be the splitting field of a separable polynomial over the field K and $G = Gal(F/K)$. Then we have the series of groups and fields,

$$G > G_1 > G_2 > \ldots > G_i > \ldots > \{e\}$$
$$F > F_1 > F_2 > \ldots > F_j > \ldots > K, \text{ where,}$$

1) *For H a subgroup of G, the corresponding subfield is F^H and $H = Gal(F/F^H)$.*

2) *If F^H is a subfield of F containing K, the corresponding subgroup of G is $Gal(F/F^H) = H$.*

3) *There is a one-to-one reversing correspondence between the subgroups of G and the subfields of F that contain K.*

4) *For any subgroup H of G,*

$$[F : F^H] = |H|, \text{ and,}$$
$$[F^H : K] = [G : H]$$

5) *The subgroup H is normal if and only if the subfield F^H is a normal extension of K and in this case,*

$$Gal(F^H/K) \cong Gal(F/K)/Gal(F/F^H)$$

Proof. 1) Using Corollary 96, page 183, since F is an extension field of F^H and H is a subgroup of $G = Gal(F/K)$ and so is finite, then,

$$H = Gal(F/F^H). \tag{12.2.1}$$

2) Given a subfield F^H such that $F \supseteq F^H \supseteq K$ then F is also a splitting field over F^H, so by Theorem 93, page 177, $F^{Gal(F/F^H)} = F^H$ giving $Gal(F/F^H) = H$.

3) Let $\Omega : H \to F^H = F^{Gal(F/F^H)}$.
Then by 1) and 2) we have an inverse function,

$$\Omega^{-1} : F^H \to H = Gal(F/F^H).$$

By Lemma 6, page 38, the existence of an inverse means Ω defines a one-to-one correspondence. This correspondence reverses the order in the chains of subgroups and subfields since if $L \subseteq H$ are subgroups of the Galois group G then the subfield left fixed by H is certainly contained in the subfield left fixed by L. Put simply, the more automorphisms there are, the smaller the number of elements that will be fixed by all of them.

4) First, by Corollary 89, page 166,

$$|Gal(F/F^H)| = [F : F^H] \tag{12.2.2}$$

By (12.2.1) above,

$$H = Gal(F : F^H) \tag{12.2.3}$$

Then, combining 12.2.2 and 12.2.3,

$$|H| = [F : F^H], \tag{12.2.4}$$

which proves the first statement.

*****

Second, by Theorem 83, page 154,

$$[F : K] = [F : F^H] \cdot [F^H : K] \tag{12.2.5}$$

and by Corollary 89, page 166, with $G = Gal(F/K)$,

$$|G| = [F : K] \tag{12.2.6}$$

Hence, using (12.2.5),

$$|G| = [F : F^H][F^H : K] \tag{12.2.7}$$

By Lagrange's Theorem 23, page 64,

$$|G| = |H| \cdot [G : H] \tag{12.2.8}$$

Hence, (12.2.7) and (12.2.8) give,

$$|H|[G : H] = [F : F^H][F^H : K] \tag{12.2.9}$$

Then, using (12.2.4),

$$[F : F^H][G : H] = [F : F^H][F^H : K]$$

so by cancellation,

$$[G : H] = [F^H : K]$$

proving the second statement.

5) We want to show the subgroup H is normal if and only if the subfield F^H is a normal extension of K and in this case,

$$Gal(F^H/K) \cong Gal(F/K)/Gal(F/F^H)$$

We first claim that if a subgroup H in the chain of groups is a normal subgroup of $G = Gal(F/K)$, then,

$$Gal(F^H/K) \cong Gal(F/K)/Gal(F/F^H).$$

We will prove this by defining a group homomorphism that leads to a normal subgroup and then we will use it to prove the isomorphism.
We have the setup that $K \subseteq F^H \subseteq F$ is a tower of fields where F is the splitting field of some polynomial $f(x) \in K[x]$ and F^H is a subfield of F.
Let,

$$\Psi : Gal(F/K) \to Gal(F^H/K),\ \Psi(\phi) = \phi|_{F^H}$$

where $\phi \in Gal(F/K)$ and $\phi|_{F^H}$ means ϕ is restricted to acting only on the elements of F^H.
Then Ψ is a group homomorphism under composition of functions since if $\sigma, \tau \in Gal(F/K)$ and $a \in F^H$ then,

$$\begin{aligned}
\Psi(\sigma \circ \tau(a)) &= \Psi\sigma\tau(a) \\
&= (\sigma\tau)|_{F^H}(a) \\
&= \sigma\tau(a)\ since\ a \in F^H \\
&= \sigma(\tau(a)) \\
&= \sigma|_{F^H}(\tau|_{F^H}(a)) \\
&= \Psi(\sigma)(\Psi(\tau)(a)) \\
&= \Psi(\sigma) \circ \Psi(\tau)(a)
\end{aligned}$$

Now by Definition 34, page 73,

$$\begin{aligned} ker(\Psi) &= \{\phi \mid \phi \in Gal(F/K) \mid \Psi(\phi) = id\},\ id \text{ the identity automorphism on } F^H. \\ &= \{\phi \mid \phi \in Gal(F/K) \mid \phi|_{F^H} = id\} \end{aligned}$$

So $\phi \in ker(\Psi)$ if and only if $\phi|_{F^H}$ is the identity automorphism on F^H, that is $\phi(a) = a$ for all $a \in F^H$. But then, $\phi \in Gal(F/F^H)$.
Hence, again by definition, $ker(\Psi) = Gal(F/F^H)$.
But by Theorem 87 above, the kernel of a group is a normal subgroup of that group. So we are in the situation required for the assumption, namely,

$$H = Gal(F/F^H) \lhd Gal(F/K).$$

But then, since F is the splitting field of a polynomial over K by Theorem 93, page 177, each automorphism $\phi \in F^H$ extends to an element of $Gal(F/K)$ and therefore ψ is onto and[8] $\psi(Gal(F/K)) = Gal(F^H/K)$. We have therefore proved the claim, since, by the First Isomorphism Theorem 33, page 73,

$$Gal(F/K)/Gal(F/F^H) \cong Gal(F^H/K)$$

*****

We now proceed to prove the "if and only if" statements in (5).
First, assume $H = Gal(F/F^H)$ whose automorphisms fix all the elements of F^H, is a normal subgroup of $Gal(F/K)$. We want to show F^H is a normal field extension of K. By Theorem 95, page 181, we only need to show F^H is a splitting field over K of a polynomial with coefficients in K.
Since $H = Gal(F/F^H)$ is a normal subgroup of $Gal(F/K)$ then if $\tau \in Gal(F/K)$ and $\sigma \in H$, then $\tau^{-1}\sigma\tau \in H$ which means $\tau^{-1}\sigma\tau$ fixes all the elements of F^H, so for all $a \in F^H$,

$$\begin{aligned} &\tau^{-1}\sigma\tau(a) = a \\ &\Rightarrow \tau\tau^{-1}\sigma\tau(a) = \tau(a) \\ &\Rightarrow \sigma\tau(a) = \tau(a) \end{aligned}$$

or σ fixes $\tau(a)$. Therefore since,

$$F^{Gal(F/F^H)} = \{a \in F \mid \sigma(a) = a \text{ for all } \sigma \in Gal(F/F^H)\},\ \text{by (12.2.1)}$$

this means,

$$\tau(a) \in F^{Gal(F/F^H)} = F^H.$$

[8] See Note 15, page 74

Now F^H is a finite separable extension of K since F is and $F^H \subseteq F$. So, by Theorem 91, page 173, $F^H = K(\gamma)$ for some $\gamma \in F^H$. Let $p(x)$ be the minimal polynomial of γ over K.
By Theorem 95, page 181, all the zeros of $p(x)$ belong to F. If b is any zero of $p(x)$ then by Theorem 86[9], there is an automorphism $\tau \in Gal(F/K)$ with $b = \tau(a)$. But we have just shown $\tau(a) \in F^H$ for all $a \in F^H$ and $\tau \in Gal(F/K)$. Therefore $b \in F^H$.
So all the zeros of $p(x)$ belong to F^H making F^H the splitting field of a polynomial $p(x)$ over K and hence F^H is a normal extension of K.

*****

Second, to prove the converse, we assume F^H is a normal extension of K.
We need to prove that for all $\phi \in Gal(F/K)$ and $\theta \in Gal(F/F^H)$ that $\phi^{-1}\theta\phi \in Gal(F/F^H)$ so that $H = Gal(F/F^H)$ is a normal subgroup[10] of $G = Gal(F/K)$. Let F^H be a normal extension of K and let $\phi \in Gal(F/K)$.
If $p(x)$ is the minimal polynomial of $\gamma \in F^H$ then $\phi(\gamma)$ is also a root of $p(x)$ and so we must have $\phi(\gamma) \in F^H$ since F^H is a normal extension of K.[11]
Thus for any $\theta \in Gal(F/F^H)$ we have $\theta\phi(\gamma) = \phi(\gamma) = \gamma$, that is θ fixes the elements of F^H and so,

$$\phi^{-1}\theta\phi(\gamma) = \phi^{-1}\phi(\gamma) = \gamma$$

or $\phi^{-1}\theta\phi$ fixes γ and therefore $\phi^{-1}\theta\phi \in Gal(F/F^H)$, making $H = Gal(F/F^H)$ a normal subgroup of $G = Gal(F/K)$ by Definition 31, page 65.

□

12.3 Examples of Fundamental Theorem of Galois Theory

Example 95. *Consider* $f(x) = x^4 - 5x^2 + 6 = (x^2 - 2)(x^2 - 3)$.
The roots are $\pm\sqrt{2}, \pm\sqrt{3}$. *The extension field containing all the roots is*

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}.$$

The Galois group of $f(x)$ *over* $\mathbb{Q}$ *is the set of automorphisms that permute* $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ *and therefore specifically* $\sqrt{2}, \sqrt{3}, \sqrt{6}$ *while leaving fixed all* $a \in \mathbb{Q}$.

[9] The automorphisms permute the roots - see Theorem 86, page 162
[10] By Definition 31 on page 65.
[11] That is, any polynomial with a root in F^H is a product of linear factors in F^H.

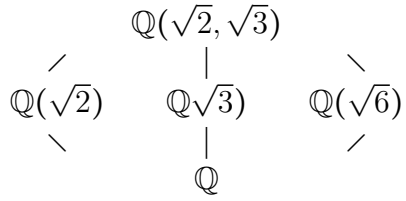
As we found earlier in Example 86, page 167, they are:

$$\begin{aligned}
i &: \sqrt{2} \to \sqrt{2}, \sqrt{3} \to \sqrt{3}, \sqrt{6} \to \sqrt{6}, \textit{the identity map fixing all elements} \\
\alpha &: \sqrt{2} \to -\sqrt{2}, \sqrt{3} \to \sqrt{3}, \sqrt{6} \to -\sqrt{6}, \textit{fixing } \sqrt{3} \textit{ only} \\
\beta &: \sqrt{2} \to \sqrt{2}, \sqrt{3} \to -\sqrt{3}, \sqrt{6} \to -\sqrt{6}, \textit{fixing } \sqrt{2} \textit{ only} \\
\gamma &: \sqrt{2} \to -\sqrt{2}, \sqrt{3} \to -\sqrt{3}, \sqrt{6} \to \sqrt{6}, \textit{fixing } \sqrt{6} \textit{ only}
\end{aligned}$$

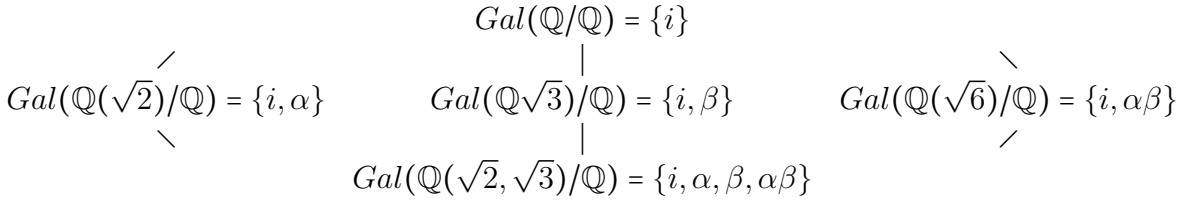
Note, $\gamma = \alpha\beta$ *since,*

$$\begin{aligned}
\alpha\beta(\sqrt{2}) &= \alpha(\sqrt{2}) = -\sqrt{2} \\
\alpha\beta(\sqrt{3}) &= \alpha(-\sqrt{3}) = -\sqrt{3} \\
\alpha\beta(\sqrt{6}) &= \alpha(-\sqrt{6}) = \sqrt{6}
\end{aligned}$$

We conclude the Galois group $Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \{i, \alpha, \beta, \alpha\beta\}$
We can set up a one-to-one reversing correspondence between the subgroups of the Galois group and the subfields of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$*, reversing in the sense that the larger the subgroup, the smaller the corresponding subfield. The two lattices of groups and fields are as shown below.*



Subfields



Subgroups

In the language of the theorem, there is a one-to-one reversing correspondence between the subgroups of the Galois group $Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3})$ *and the subfields of the splitting field* $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ *of the polynomial* $f(x) = x^4 - 5x^2 + 6 = (x^2 - 2)(x^2 - 3)$ *over* $\mathbb{Q}$*.*

Recall that the symbol F^G is the G–fixed subfield of F, that is,

$$F^G = \{a \in F \mid \phi(a) = a \text{ for all } \phi \in G\}$$

Then, in particular, we have the theorem statements demonstrated in our example as shown.

a. *Theorem statements (1) and (2):*
If H is a subgroup of G then the corresponding subfield is F^H and conversely, if F^H is a subfield of F that contains K then the corresponding subgroup of G is $Gal(F/F^H)$ and $F^H = F^{Gal(F/F^H)}$.

In our example $G = \{i, \alpha, \beta, \alpha\beta\}$ and we have,

1) *$\{i\}$ is a subgroup of G and the corresponding subfield is $F^{\{i\}} = \{a \in F \mid \phi(a) = a \text{ for all } \phi \in G\}$ which is simply F or $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $\{i\} = Gal(F/F^{\{i\}})$.*
2) *$G = \{i, \alpha, \beta, \alpha\beta\}$ is a subgroup of G and the corresponding subfield is F^G which is just $\mathbb{Q}$ since only $\mathbb{Q}$ is fixed by all the automorphisms.*
3) *$\{i, \alpha\}$ is a subgroup of G and the corresponding subfield is $F^{\{i,\alpha\}}$ which is $\mathbb{Q}(\sqrt{2})$ since only $\mathbb{Q}(\sqrt{2})$ is fixed by all the automorphisms in $\{i, \alpha\}$*
4) *$\{i, \beta\}$ is a subgroup of G and the corresponding subfield is $F^{\{i,\beta\}}$ which is $\mathbb{Q}(\sqrt{3})$ since only $\sqrt{3}$ is fixed by all the automorphisms in $\{i, \beta\}$*
5) *$\{i, \alpha\beta\}$ is a subgroup of G and the corresponding subfield is $F^{\{i,\alpha\beta\}}$ which is $\mathbb{Q}(\sqrt{6})$ since only $\sqrt{6}$ is fixed by all the automorphisms in $\{i, \alpha\beta\}$*

b. *Theorem statement (4):*
For any subgroup H of G, $[F : F^H] = |H|$ and $[F^H : K] = [G : H]$.

To illustrate $[F : F^H] = |H|$ in our example consider the case $H = \{i, \alpha\}$. Then $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ since for this the minimal polynomial is $x^2 - 2$ which has degree 2 and $|H| = |\{i, \alpha\}| = 2$.

*****

To illustrate $[F^H : K] = [G : H]$ in our example, first note $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ since the minimal polynomial $x^2 - 2$ has degree 2. Now the factor group,

$$\begin{aligned}\{i, \alpha, \beta, \alpha\beta\}/\{i, \alpha\} &= \{i\{i, \alpha\}, \alpha\{i, \alpha\}, \beta\{i, \alpha\}, \alpha\beta\{i, \alpha\}\} \\ &= \{\{i, \alpha\}, \{\alpha, \alpha^2\}, \{\beta, \alpha\beta\}, \{\alpha\beta, \alpha^2\beta\} \\ &= \{\{i, \alpha\}, \{\beta, \alpha\beta\}\} \text{ since } \alpha^2 = i.\end{aligned}$$

So the number of cosets,

$$[\{i, \alpha, \beta, \alpha\beta\} : \{i, \alpha\}] = 2 \text{ also.}$$

The other cases are similar.

c. *Theorem statement (5):*
The subgroup H is normal if and only if the subfield F^H is a normal extension of K and in this case, $Gal(F^H/K) \cong Gal(F/K)/Gal(F/F^H)$.
First, recall a subgroup H of a group G is a normal subgroup if $ghg^{-1} \in H$ for all $h \in H$ and $g \in G$. In particular, by Theorem 30, page 69, all abelian subgroups are normal subgroups.
Second, F is a normal extension of a field K if F is the splitting field over K of a separable polynomial, that is a polynomial which factors in F into simple factors (read, degree one polynomials).
In our example $H = \{i, \alpha\}$ is a normal subgroup by Theorem 30 since all groups of order 2 are abelian. The subfield $F^H = \mathbb{Q}(\sqrt{2})$ is a normal extension of $\mathbb{Q}$ since the minimal polynomial $x^2 - 2$ splits in $\mathbb{Q}(\sqrt{2})$ into two degree one factors, namely, $x - \sqrt{2}, x + \sqrt{2}$. $\diamond$

Example 96. *Consider $f(x) = x^3 - 2 \in \mathbb{Q}[x]$.*
Since by the usual factoring of the difference of two cubes,

$$f(x) = x^3 - 2 = (x^{\frac{1}{3}} - (2^{\frac{1}{3}})^3) = (x - 2^{\frac{1}{3}})(x^2 + 2^{\frac{1}{3}}x + 2^{\frac{2}{3}})$$

and, by the quadratic formula,

$$x^2 + 2^{\frac{1}{3}}x + 2^{\frac{2}{3}} = 0 \Rightarrow x = \frac{-2^{\frac{1}{3}} \pm \sqrt{2^{\frac{2}{3}} - 4 \cdot 2^{\frac{2}{3}}}}{2} = 2^{\frac{1}{3}} \cdot \frac{-1 \pm \sqrt{3}i}{2}$$
$$= 2^{\frac{1}{3}}\omega, 2^{\frac{1}{3}}\omega^2, \ \omega = \frac{-1 \pm \sqrt{3}i}{2},$$

so we can write

$$f(x) = (x - 2^{\frac{1}{3}})(x - 2^{\frac{1}{3}}\omega)(x - 2^{\frac{1}{3}}\omega^2)$$

where ω, ω^2 are the roots of the monic polynomial $x^2 + x + 1$. The three roots of $f(x)$ are therefore $2^{\frac{1}{3}}, 2^{\frac{1}{3}}\omega, 2^{\frac{1}{3}}\omega^2$.
The splitting field of $f(x)$ over $\mathbb{Q}$ is the smallest extension field that contains all the roots. We can construct it in two steps in two different ways, showing the respective minimal polynomials, thus:

$$\begin{array}{c} \mathbb{Q}(\sqrt[3]{2}, \omega) \\ p_2(x) = x^2 + x + 1 \Big| \\ \mathbb{Q}(\sqrt[3]{2}) \\ p_1(x) = x^3 - 2 \Big| \\ \mathbb{Q} \end{array} \qquad \begin{array}{c} \mathbb{Q}(\sqrt[3]{2}, \omega) \\ p_2(x) = x^3 - 2 \Big| \\ \mathbb{Q}(\omega) \\ p_1(x) = x^2 + x + 1 \Big| \\ \mathbb{Q} \end{array}$$

While in the previous example, $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}$ *this is not that simple for* $\mathbb{Q}(2^{\frac{1}{3}})$ *since for* $F = \{a + b\ 2^{\frac{1}{3}} \mid a,b \in \mathbb{Q}\}$*, as we saw in a previous example, we do not have closure under multiplication as required for a field. Thus,*

$$(a + b\ 2^{\frac{1}{3}})(c + d\ 2^{\frac{1}{3}}) = A + B\ 2^{\frac{1}{3}} + C\ 2^{\frac{2}{3}} \notin F = \{a + b2^{\frac{1}{3}} \mid a,b \in \mathbb{Q}\}$$

In any case, this would mean a basis $\mathfrak{B}$ *for* F *over* $\mathbb{Q}$ *has just two elements,* $\mathfrak{B} = \{1, 2^{\frac{1}{3}}\}$*, but the minimal polynomial has degree 3 so the basis for* F *over* $\mathbb{Q}$ *must contain 3 elements. Prompted by the result of the multiplication, we choose the basis* $\{1, 2^{\frac{1}{3}}, 2^{\frac{2}{3}}\}$ *and identify,*

$$\mathbb{Q}(2^{\frac{1}{3}}) = \{a + b\ 2^{\frac{1}{3}} + c\ 2^{\frac{2}{3}} \mid a,b,c \in \mathbb{Q}\}$$

Then,

$$\begin{aligned}\mathbb{Q}(2^{\frac{1}{3}},\omega) &= \{X + Y\omega \mid X,Y \in \mathbb{Q}(2^{\frac{1}{3}})\} \\ &= \{a + b\ 2^{\frac{1}{3}} + c\ 2^{\frac{2}{3}} + \omega(d + e\ 2^{\frac{1}{3}} + f\ 2^{\frac{2}{3}}) \mid a,b,c,d,e,f \in \mathbb{Q}\} \\ &= \{a + b\ 2^{\frac{1}{3}} + c\ 2^{\frac{2}{3}} + d\omega + e\ 2^{\frac{1}{3}}\omega + f\ 2^{\frac{2}{3}}\omega) \mid a,b,c,d,e,f \in \mathbb{Q}\}\end{aligned}$$

Therefore a basis for $\mathbb{Q}(2^{\frac{1}{3}},\omega)$ *over* $\mathbb{Q}$ *is,*

$$\mathfrak{B} = \{1, 2^{\frac{1}{3}}, 2^{\frac{2}{3}}, \omega, 2^{\frac{1}{3}}\omega, 2^{\frac{2}{3}}\omega\}$$

and $|\mathfrak{B}| = 6$ *which agrees with,*

$$[\mathbb{Q}(2^{\frac{1}{3}},\omega) : \mathbb{Q}] = [\mathbb{Q}(2^{\frac{1}{3}},\omega) : \mathbb{Q}(2^{\frac{1}{3}}] \cdot [\mathbb{Q}(2^{\frac{1}{3}} : \mathbb{Q}] = 2 \cdot 3 = 6$$

since the respective minimal polynomials have degrees 2,3 as noted above.
Further, since the order of the Galois group is given by the relationship,

$$|Gal(\mathbb{Q}(2^{\frac{1}{3}},\omega)/\mathbb{Q}| = [\mathbb{Q}(2^{\frac{1}{3}},\omega) : \mathbb{Q}] = 6,$$

the Galois group has 6 elements.
They may be identified by their action on the generating elements $2^{\frac{1}{3}},\omega$ *as follows.*

$$\begin{aligned} i &: 2^{\frac{1}{3}} \to 2^{\frac{1}{3}},\ \omega \to \omega \\ f &: 2^{\frac{1}{3}} \to 2^{\frac{1}{3}}\omega,\ \omega \to \omega \\ g &: 2^{\frac{1}{3}} \to 2^{\frac{1}{3}},\ \omega \to \omega^2 \\ f^2 &: 2^{\frac{1}{3}} \to 2^{\frac{1}{3}}\omega^2,\ \omega \to \omega \\ gf^2 &: 2^{\frac{1}{3}} \to 2^{\frac{1}{3}}\omega,\ \omega \to \omega^2 \\ gf &: 2^{\frac{1}{3}} \to 2^{\frac{1}{3}}\omega^2,\ \omega \to \omega^2 \end{aligned}$$

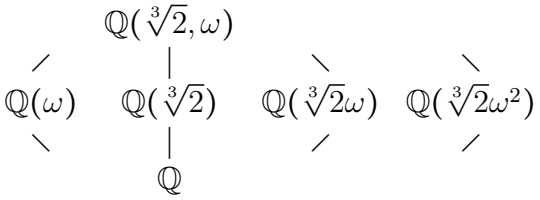
Note we have replaced the six identifiers ϕ_0 to ϕ_5 with the identity i, the letters f, g and combinations of these letters. You can easily see for example that the last automorphism is gf since,

$$g \circ f(2^{\frac{1}{3}}) = g(2^{\frac{1}{3}}\omega) = g(2^{\frac{1}{3}})g(\omega) = 2^{\frac{1}{3}}\omega^2;$$
$$g \circ f(\omega) = g(\omega) = \omega^2$$

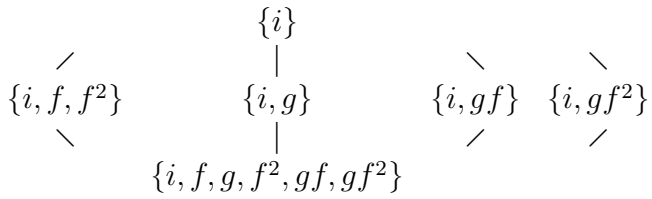
We conclude,

$$Gal(\mathbb{Q}(2^{\frac{1}{3}}, \omega)/\mathbb{Q}) = \{i, f, f^2, g, gf, gf^2\}$$

Let us now consider the two lattices of subgroups and field extensions. We have,



Subfields



Subgroups

The subgroups of the Galois group G and the corresponding subfields are as follows:

1. $G \to \mathbb{Q}$
2. $\{i\} \to \mathbb{Q}(\sqrt[3]{2}, \omega)$
3. *There is a unique subgroup of order 3, namely, $\{i, f, f^2\}$, which is cyclic since $f^3 = i$ and therefore normal by Theorem 30, page 69. This is so since if,*

   (a) $f^3(\sqrt[3]{2}) = f^2(f(\sqrt[3]{2})) = f^2(\sqrt[3]{2}\omega) = f(f(\sqrt[3]{2})f(\omega))$
   $= f(\sqrt[3]{2}\omega \cdot \omega) = \sqrt[3]{2}\omega^3 = \sqrt[3]{2}$

   (b) $f^3(\omega) = f^2(\omega) = f(\omega) = \omega$

   then $f^3 = i$, the identity.
   This corresponds to the fact that the corresponding subfield $\mathbb{Q}(\omega)$ is a normal or Galois extension[12] of $\mathbb{Q}$ since the minimal polynomial $x^2 + x + 1$ factors into linear factors as $x^2 + x + 1 = (x + \omega)(x + \omega^2)$.

[12] See Definition 71, page 172

4. *There are three subgroups of order 2, namely* $\{i, g\}, \{i, gf\}, \{i, gf^2\}$ *corresponding to the three subfields* $\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{2}\omega), \mathbb{Q}(\sqrt[3]{2}\omega^2)$. *These subgroups are not normal in the Galois group and this corresponds to the fact that the subfields are neither normal nor separable.*
For example, to show $\{i, g\}$ *is not normal in* $\{i, f, g, f^2, gf, gf^2\}$ *it suffices to show* $\alpha\beta\alpha^{-1} \notin \{i, g\}$ *for any* $\alpha \in \{i, f, g, f^2, gf, gf^2\}$ *and* $\beta \in \{i, g\}$.
Given $f^3 = f^2 \cdot f = 1$ *we choose* $\alpha = f^2$ *so that* $\alpha^{-1} = f$ *and then,*

$$f^2gf(\sqrt[3]{2}) = f^2g(\sqrt[3]{2}\omega) = f^2(\sqrt[3]{2}\omega^2) = f(\sqrt[3]{2}\ \omega \cdot \omega \cdot \omega) = f(\sqrt[3]{2}) = \sqrt[3]{2}\omega \neq g(\sqrt[3]{2})$$

or the identity, so $f^2gf \notin \{i, g\}$.
The other two arguments are similar. The reason why the corresponding subfields are not normal extensions is that each contains only a single root of its monic polynomial $x^3 - 2$. *To be a normal extension any polynomial with roots in* $\mathbb{Q}(\sqrt[3]{2})$ *must split completely in* $\mathbb{Q}(\sqrt[3]{2})$.

*****

Finally, we have the theorem statement that if the subgroup H *is normal, then,*

$$Gal(F^H/K) \cong Gal(F/K)/Gal(F/F^H)$$

In our example $K = \mathbb{Q}$. *We have already shown in 3. above that* $H = \{i, f, f^2\}$ *is a normal subgroup of* $Gal(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$. *Then, given* $F^H = \mathbb{Q}(\omega)$, *it remains to show,*

$$Gal(\mathbb{Q}(\omega)/\mathbb{Q}) \cong Gal(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})/Gal(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}(\omega))$$

We first note $Gal(\mathbb{Q}(\sqrt[3]{2}, \omega)$ *is non-abelian. We only need one counter example so consider,*

$$f : \sqrt[3]{2} \to \sqrt[3]{2}\omega,\ \omega \to \omega;$$
$$g : \sqrt[3]{2} \to \sqrt[3]{2},\ \omega \to \omega^2$$

Then,

$$f \circ g(\sqrt[3]{2}) = f(\sqrt[3]{2}) = \sqrt[3]{2}\omega$$
but
$$g \circ f(\sqrt[3]{2}) = g(\sqrt[3]{2}, \omega) = \sqrt[3]{2}\omega^2 \neq f \circ g(\sqrt[3]{2}),$$

so $Gal(\mathbb{Q}(\sqrt[3]{2}, \omega)$ *is non-abelian.*
Since the Galois group is of order 6 and is non-abelian, we conclude it is isomorphic to the symmetric group S_3 *which is also non-abelian and of order 6. That* S_3 *is non-abelian can also be shown by a single counter example, say,*

$$(12)(13)(2) = 1$$
but
$$(13)(12)(2) = 3$$

Let us again consider the tower of fields and respective minimal polynomials,

$$\begin{array}{c} \mathbb{Q}(\sqrt[3]{2},\omega) \\ \Big| \\ p_2(x) = x^3 - 2 \\ \Big| \\ \mathbb{Q}(\omega) \\ \Big| \\ p_1(x) = x^2 + x + 1 \\ \Big| \\ \mathbb{Q} \end{array}$$

Since $\mathbb{Q}(\sqrt[3]{2},\omega)$ *is the splitting field of the degree 3 polynomial* $x^3 - 2$ *over* $\mathbb{Q}(\omega)$ *and,*

$$|Gal(\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q}(\omega))| = [\mathbb{Q}(\sqrt[3]{2},\omega) : \mathbb{Q}(\omega)] = 3,$$

then,

$$Gal(\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q}(\omega)) \cong A_3$$

where A_3 *is the alternating group of three elements and is a normal subgroup of* S_3*. Similarly,* $\mathbb{Q}(\omega)$ *is the splitting field of the degree 2 polynomial* $x^2 + x + 1$ *over* $\mathbb{Q}$ *so,*

$$|Gal(\mathbb{Q}(\omega)/\mathbb{Q}))| = [\mathbb{Q}(\omega) : \mathbb{Q}] = 2$$

making,

$$Gal(\mathbb{Q}(\omega)/\mathbb{Q}) \cong \mathbb{Z}_2.$$

Then, since we already know from Theorem 36 on page 78 that $S_3/A_3 \cong \mathbb{Z}_2$*, we have shown,*

$$Gal(\mathbb{Q}(\omega)/\mathbb{Q}) \cong Gal(\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q})/Gal(\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q}(\omega))$$

Chapter 13

Insolvability of Higher Degree Polynomials

Which brings us to our goal, to prove the quintic, and in general, polynomials of degree ≥ 5, are not solvable by radicals.

13.1 Preamble to the Main Theorem

The two roots of the irreducible polynomial equation $f(x) = ax^2 + bx + c = 0$, $a, b, c \in \mathbb{Q}$ are,

$$x_1 = -\frac{b}{2a} + \frac{\sqrt{b^2 - 4ac}}{2a},\ x_2 = -\frac{b}{2a} - \frac{\sqrt{b^2 - 4ac}}{2a}$$

Let u be such that $u^2 = b^2 - 4ac \in \mathbb{Q}$. If we construct the tower of fields,

$$\begin{array}{c} \mathbb{Q}(u) \\ | \\ u^2 \in \mathbb{Q} \end{array}$$

then $\mathbb{Q}(u) = \{c + du \mid c, d \in \mathbb{Q}\}$ contains the splitting field (all solutions) of $f(x)$ as we easily see by letting $c = -\frac{b}{2a},\ d = \frac{\pm 1}{2a}$. Note the extension field is obtained by adjoining an element whose square belongs to the field below it. Of course we may have $b^2 - 4ac < 0$ in which case we write $\sqrt{b^2 - 4ac} = \sqrt{-(b^2 - 4ac)}i$ and the splitting field needs to be $\mathbb{Q}(u, i)$ where $i = \sqrt{-1}$ is a second root of unity giving for full completeness the tower,

$$\begin{array}{c} \mathbb{Q}(u, i) \\ | \\ \mathbb{Q}(u) \\ | \\ u^2 \in \mathbb{Q} \end{array}$$

Similarly, we found on page 16 a formula for the three roots of the cubic $f(y) = y^3 + py + q$, namely,

$$y_1 = \sqrt[3]{Q},\ y_2 = \sqrt[3]{Q}\omega,\ y_3 = \sqrt[3]{Q}\omega^2$$

where $\omega = e^{\frac{2\pi i}{3}},\ Q = -\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^2}$

Let u_1, u_2 be such that $u_1^2 = \left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^2 \in \mathbb{Q},\ u_2^3 = -\left(\frac{q}{2}\right) + u_1 \in \mathbb{Q}(u_1)$.
If we construct the tower of fields,

$$\begin{array}{c} \mathbb{Q}(u_1, u_2, \omega) = \{e + f\omega \mid e, f \in \mathbb{Q}(u_1, u_2)\} \\ | \\ \mathbb{Q}(u_1, u_2) = \{c + du_2 \mid c, d \in \mathbb{Q}(u_1)\} \\ | \\ u_2^3 \in \mathbb{Q}(u_1) = \{a + bu_1 \mid a, b \in \mathbb{Q}\} \\ | \\ u_1^2 \in \mathbb{Q} \end{array}$$

then $\mathbb{Q}(u_1, u_2, \omega)$ contains the splitting field of $f(y)$. Note each extension field is obtained by adjoining an element whose square or cube belongs to the field below it. Finally we create the top extension field by adding the third roots of unity.

In both of the polynomials $f(x) = ax^2 + bx + c,\ f(y) = x^3 + px + q$, we found an extension field which contains the elements that could be assembled as a formula for the roots of the polynomial. The formulas contained only rational numbers combined by the field operations (addition, multiplication, inverses) and taking n^{th} roots as well as the n^{th} roots of unity where n is the degree of the respective minimal polynomials linking the subfields. Accordingly we say the two equations can be solved by radicals. Hence to show no such formulas exist for polynomials of degree ≥ 5 we need to show, for polynomials of degree ≥ 5, we cannot have an extension field that contains the elements that could be assembled as a formula for the roots of the polynomial.

Formally, we define,

Definition 78. *radical extension field*
An extension field F of the base field $\mathbb{Q}$ is a radical extension of $\mathbb{Q}$ if there exist elements $u_1, u_2, \ldots, u_m \in F$ such that,

1. $F = \mathbb{Q}(u_1, u_2, \ldots, u_m)$
2. $u^{n_1} \in \mathbb{Q}$ *and* $u_i^{n_i} \in \mathbb{Q}(u_1, u_2, \ldots, u_{i-1})$ *for* $n_i \in \mathbb{Z}$ *for* $1 \leq i \leq m$.

In essence each extension field contains one more n^{th} root of an element taken from $u_1, u_2, \ldots, u_n \in F$. Accordingly we define,

Definition 79. *solvable by radicals*
For a polynomial $f(x) \in \mathbb{Q}[x]$, the equation $f(x) = 0$ is said to be solvable by radicals if there exists a radical extension F of $\mathbb{Q}$ that contains all the roots of $f(x)$.

The key idea in building the radical extension is the adding in of roots of the polynomial $x^n - a$ for suitable values of a since $p(x) = x^n - a$ is the minimal polynomial of each $\sqrt[n]{a}$. Finally we find we need to add in only one root of unity carefully constructed.

Accordingly, we first need to determine the structure of the Galois Group of the polynomial of the form $x^n - a$ and then use the Fundamental Theorem of Galois Theory to see what happens when we one-by-one adjoin the roots of $x^n - a$ to the base field $\mathbb{Q}$.

We start with $x^n - 1 \in \mathbb{Q}[x]$. There are n solutions of the equation $x^n = 1$, we call them the n^{th} roots of unity.[1]

Making use of Euler's result, (see the Appendix),

$$e^{\pi i} = -1 \Rightarrow e^{2\pi i} = 1,$$

we have

$$\sqrt[n]{1} = \left(e^{2\pi i}\right)^{\frac{1}{n}} = e^{\frac{2\pi i}{n}}$$

but we can extend this into n different roots of unity by noting $e^{\frac{2\pi i}{n}k} = \left(e^{\frac{2\pi i}{n}}\right)^k = 1$ and that for $k = 0, 1, \ldots, n-1$ each value of $e^{\frac{2\pi i}{n}k}$ is different but then repetition begins and continues.

Example 97. *Thus, for example, the fifth roots of unity are the set $\{e^0, e^{\frac{2\pi i}{5}\cdot 1}, e^{\frac{2\pi i}{5}\cdot 2}, e^{\frac{2\pi i}{5}\cdot 3}, e^{\frac{2\pi i}{5}\cdot 4}\}$ and there are no more since, for example,*

$$e^{\frac{2\pi i}{5}\cdot 7} = e^{\frac{2\pi i}{5}\cdot 2} \times e^{\frac{2\pi i}{5}\cdot 2} = e^{\frac{2\pi i}{5}\cdot 2}. \qquad \diamond$$

We prove in Theorem 99 that the roots of unity form a group under multiplication.

[1] See the appendix for the discussion of the roots of unity resulting from the equation $x^n - 1 = 0 \Rightarrow x^n = 1 \Rightarrow x = \sqrt[n]{1}$.

Theorem 99. ***
The n^{th} roots of unity form a cyclic group under multiplication modulo n.

Proof. The n^{th} roots of unity are,

$$\{e^{2\pi i\frac{k}{n}} \mid 1 \le k \le n\} = \{e^{2\pi i\frac{1}{n}}, e^{2\pi i\frac{2}{n}}, \ldots, e^{2\pi i\frac{n}{n}} = 1\} =< \{e^{2\pi i\frac{1}{n}} >$$

Clearly this satisfies Definition 11, page 32, of a cyclic group generated by an element a, namely $< a > \mid a \in \mathbb{Z}\}$. It remains to be proved it is a group. But we have,

- Closure: Consider $e^{2\pi i\frac{k}{n}} \cdot e^{2\pi i\frac{j}{n}} = e^{2\pi i\frac{j+k}{n}}$. Under multiplication modulo n we can have $j + k \le n$ so the product is an element of the set.
- Identity: $e^{2\pi i\frac{n}{n}} = 1$.
- Inverses: $e^{2\pi i\frac{k}{n}} \cdot e^{2\pi i\frac{n-k}{n}} = 1$ so $e^{2\pi i\frac{k}{n}}$ has the inverse $e^{2\pi i\frac{n-k}{n}}$.
- Associativity: Obvious.

So the n^{th} roots of unity are a group. □

We then prove in Theorem 100 that if F is the splitting field of $f(x) = x^n - 1$ over $\mathbb{Q}$ then the Galois group $Gal(F/\mathbb{Q})$ is abelian

Theorem 100. ***
Let F be the spitting field of $x^n - 1$ over $\mathbb{Q}$. Then $Gal(F/K)$ is an abelian group.

Proof. The distinct roots of $x^n - 1$ are the n^{th} roots of unity,

$$\omega^0 = 1, \omega, \omega^2, \ldots, \omega^{n-1} = 1, \text{ or } \omega = e^{2\pi i\frac{k}{n}}, \ k = 0, 1, \ldots, n-1.$$

Therefore, the splitting field of $x^n - 1$ over $\mathbb{Q}$ is $F = \mathbb{Q}(\omega)$.
Since the elements ϕ_i of the Galois group permute the group of roots, (Theorem 86, page 162), we only need to observe their possible actions on the group generator ω. The only possibilities are the n automorphisms,

$$\phi_i(\omega) = \omega^k, \ 0 \le k \le n-1.$$

Then,

$$\phi_j(\omega)\phi_k(\omega) = \omega^j\omega^k = \omega^{j+k}$$
$$\phi_k(\omega)\phi_j(\omega) = \omega^k\omega^j = \omega^{j+k}$$

shows the Galois group is abelian. □

We prove for F the splitting field of $x^n - a$ over $\mathbb{Q}$ that $Gal(F/\mathbb{Q})$ is a cyclic group.

Theorem 101. ***
Let $a \in \mathbb{Q}$ and F be the spitting field of $x^n - a$ over $\mathbb{Q}$. Then $Gal(F/\mathbb{Q})$ is a cyclic group whose order is a divisor of n.

Proof. The n distinct roots of $x^n - a$ are $\sqrt[n]{a} = a^{\frac{1}{n}}$ multiplied by the n^{th} roots of unity, namely,

$$a^{\frac{1}{n}}\omega,\ \omega = e^{\frac{2k\pi i}{n}},\ 0 \le k \le n-1.$$

Therefore, the splitting field of $x^n - a$ over $\mathbb{Q}$ is $F = \mathbb{Q}(a^{\frac{1}{n}}, \omega)$.
Since the elements ϕ_k of the Galois group permute the roots, we only need to observe their possible actions on $a^{\frac{1}{n}}\omega$. The only possibilities are the n automorphisms,

$$\phi_k(a^{\frac{1}{n}}\omega) = a^{\frac{1}{n}}\omega^k,\ 0 \le k \le n-1.$$

Consider,

$$\Omega : Gal(F/\mathbb{Q}) \to \mathbb{Z}_n \text{ where } \Omega(\phi_k(a^{\frac{1}{n}}\omega)) = k,\ 0 \le k \le n-1.$$

The homomorphism step is as follows.

$$\begin{aligned}\Omega(\phi_k \circ \phi_j)(a^{\frac{1}{n}}\omega) &= \Omega(\phi_k(a^{\frac{1}{n}}\omega^j)) \\ &= \Omega(a^{\frac{1}{n}}\omega^{jk}) \\ &= jk \\ &= \Omega(\phi_j(a^{\frac{1}{n}}\omega))\Omega(\phi_k(a^{\frac{1}{n}}\omega))\end{aligned}$$

So Ω is a homomorphism. Clearly Ω is a one-to-one correspondence since each element of $Gal(F/K)$ is numbered exactly the same as an element of $\mathbb{Z}_n$.
Then, $Gal(F/\mathbb{Q}) \cong \mathbb{Z}_n$ and since $\mathbb{Z}_n$ is cyclic then, by Theorem 20, page 58, so is $Gal(F/\mathbb{Q})$. □

13.2 Main Theorem

We are almost ready for our main theorem where we find the conditions under which a polynomial equation has or does not have a formula for determining its roots.
First, in Theorem 102 we prove that if E is a radical extension of $\mathbb{Q}$ then there exists an extension F of E that is a normal[2] radical extension of $\mathbb{Q}$.

[2]For F/K, F is a normal extension of K if every irreducible polynomial in $K[x]$ that contains a root in F is the product of linear factors in $F[x]$.

Theorem 102. *****
If E is a radical extension of $\mathbb{Q}$ then there exists an extension F of E that is a normal, radical extension of $\mathbb{Q}$.

Proof. Let E be a radical extension of $\mathbb{Q}$ with elements $u_1, u_2, \ldots, u_m \in E$ such that,

1. $F = \mathbb{Q}(u_1, u_2, \ldots, u_m)$
2. $u^{n_1} \in \mathbb{Q}$ and $u_i^{n_i} \in \mathbb{Q}(u_1, u_2, \ldots, u_{i-1})$ for $n_i \in \mathbb{Z}$ for $1 \leq i \leq m$.

Then, diagrammatically, Definition 78, page 198 of a radical extension is shown in Tower A of fields,

$$\begin{array}{c} E = \mathbb{Q}(u_1, \ldots, u_m) \\ | \\ u_m^{n_m} \in \mathbb{Q}(u_1, \ldots, u_{m-1}) \\ | \\ \vdots \\ | \\ u_3^{n_3} \in \mathbb{Q}(u_1, u_2) \\ | \\ u_2^{n_2} \in \mathbb{Q}(u_1) \\ | \\ u_1^{n_1} \in \mathbb{Q} \end{array}$$

Tower A

Let,

$$f(x) = (x - u_1)(x - u_2)\cdots(x - u_m) \tag{13.2.1}$$

Let F be the splitting field of $f(x)$ over $\mathbb{Q}$. This gives the tower of fields,

$$\begin{array}{c} F = \mathbb{Q}(u_1, \ldots, u_m) \\ | \\ \mathbb{Q}(u_1, \ldots, u_{m-1}) \\ | \\ \vdots \\ | \\ \mathbb{Q}(u_1) \\ | \\ \mathbb{Q} \end{array}$$

Tower B

But we can then form Tower C below.

$$
\begin{array}{c}
F = \mathbb{Q}(u_1, \ldots, u_m) \\
| \\
u_m^{n_m} \in \mathbb{Q}(u_1, \ldots, u_{m-1}) \\
| \\
\vdots \\
| \\
u_2^{n_2} \in \mathbb{Q}(u_1) \\
| \\
u_1^{n_1} \in \mathbb{Q}
\end{array}
$$

Tower C

Now, with respect to $f(x)$, every automorphism $\phi \in Gal(F/\mathbb{Q})$ permutes the roots of $f(x)$ so we can write,

$$f(x) = (x - \phi(u_1))(x - \phi(u_2))\cdots(x - \phi(u_m)) \tag{13.2.2}$$

where the factors in (13.2.2) are a permutation or rearrangement of the factors in (13.2.1).
Then each root of $f(x)$ has the form $\phi(u_i)$ for some integer i and some automorphism $\phi \in Gal(F/\mathbb{Q})$,
Since for any $\phi \in Gal(F/\mathbb{Q})$ we have $\phi(u_i^{n_i}) = \phi(u_i)^{n_i}$, we can replace each of the $u_i^{n_i}$ elements in Tower C with $\phi(u_i)^{n_i}$.
Then we have $\phi(u_i)^{n_i} \in \mathbb{Q}(\phi(u_1), \ldots, \phi(u_{n-i}))$ for $i = 2, \ldots, m$, thus enabling us to create Tower D.

$$
\begin{array}{c}
F = \mathbb{Q}(\phi(u_1), \ldots, \phi(u_m)) \\
| \\
\phi(u_m)^{n_m} \in \mathbb{Q}(\phi(u_1), \ldots, \phi(u_{m-1})) \\
| \\
\vdots \\
| \\
\phi(u_2)^{n_2} \in \mathbb{Q}(\phi(u_1)) \\
| \\
\phi(u_1)^{n_1} \in \mathbb{Q}
\end{array}
$$

Tower D

Accordingly, as is clear by comparing Tower D with the diagrammatic definition of a radical extension shown in Tower A, if $Gal(F/\mathbb{Q}) = \{\phi_1, \phi_2, \ldots, \phi_k\}$ then the elements $\{\phi_j(u_i)\}$ for $i = 1, 2, \ldots, m$ and $j = 1, 2, \ldots, k$ satisfy the conditions of the definition of a radical extension showing F is a radical extension of $\mathbb{Q}$. □

Finally, we need Theorem 103 from group theory that proves a factor group of a cyclic group is cyclic and also the definition of a primitive root of unity.

Theorem 103. ** *The factor group of a cyclic group is cyclic.*

Proof. Suppose $G =< a >= \{a^n \mid n \in \mathbb{Z}\}$.
Let G/H be any factor group of G.
We need to prove $G/H = \{(aH)^n \mid n \in \mathbb{Z}\} =< aH >$.
Now, any element of G/H is of the form gH where $g \in G$.
Since G is cyclic, there is an integer n such that $g = a^n$.
So $gH = a^nH$.
Now $a^nH = (aH)^n$ according to Definition 32, page 68, of coset multiplication.
Therefore $gH = (aH)^n,\ n \in \mathbb{Z}$ for any coset gH making,

$$G/H = \{gH \mid g \in G\} \Leftrightarrow G/H = \{(aH)^n \mid n \in \mathbb{Z}\} =< aH >$$

or G/H is cyclic. □

We further discuss roots of unity in the appendix. We distinguish the following.

Definition 80. *primitive root of unity*
ω is a primitive n^{th} root of unity if $\omega^n = 1$ but $\omega^r \neq 1$ for all $r < n$.

Example 98. *For example, consider the 6^{th} roots of unity given by $e^{2\pi i\frac{k}{6}},\ k = 0, 1, 2, 3, 4, 5$. Clearly*

$$\left(e^{2\pi i\frac{5}{6}}\right)^6 = e^{2\pi i\frac{5}{1}} = (e^{2\pi i})^5 = 1$$

but $\left(e^{2\pi i\frac{5}{6}}\right)^r \neq 1$ for any $r < 6$, making $e^{2\pi i\frac{5}{6}}$ a primitive 6^{th} root of unity.
But not all the roots of unity are primitive, since, for example,

$$\left(e^{2\pi i\frac{3}{6}}\right)^2 = e^{2\pi i} = 1 \text{ but } 2 < 6. \qquad \diamond$$

A simple investigation soon makes it clear that $e^{2\pi i\frac{k}{n}}$ is a primitive n^{th} root if and only if the fraction $\dfrac{k}{n}$ is in lowest terms, i.e. that is $gcd(k, n) = 1$.

We have done a lot of preparation. We are now ready for the main theorem, Galois' masterpiece, from which we can easily show the insolvability of polynomial equations of degree 5 and above.

Theorem 104. ***** *(Main Theorem)*
Let $f(x) \in \mathbb{Q}[x]$. If the equation $f(x) = 0$ is solvable by radicals then the Galois group, $Gal(E/\mathbb{Q})$, of E over $\mathbb{Q}$ is solvable where E is the splitting field of $f(x)$ over $\mathbb{Q}$.

Proof. Let $f(x) \in \mathbb{Q}[x]$.
Let E be the splitting field of $f(x)$ over $\mathbb{Q}$. Note that E exists by Theorem 84, page 158.
We need to show $G = Gal(E/\mathbb{Q})$ is solvable, where, using Definition 37, page 82, a group G is solvable if we can form a finite chain of subgroups,

$$\{e\} = G_0 \leq G_1 \leq G_2 \leq \ldots \leq G_n = G$$

such that $G_i \trianglelefteq G_{i+1}$, or G_i is a normal subgroup of G_{i+1}, and the factor groups G_{i+1}/G_i are all abelian.

*****

Assume $f(x) = 0$ is solvable by radicals, that is, by Definition 79 on page 198, there exists a radical extension F of $\mathbb{Q}$ that contains all the roots of $f(x)$.
So let F be a radical extension of $\mathbb{Q}$ that contains the splitting field E of $f(x)$ over $\mathbb{Q}$. We have the tower of fields,

$$\begin{array}{c} F \\ | \\ E \\ | \\ \mathbb{Q} \end{array}$$

*****

First we show, for a given root of unity, ζ,

$$Gal(E/\mathbb{Q}) \cong Gal(F(\zeta)/\mathbb{Q})/Gal(F(\zeta)/E) \tag{13.2.3}$$

We first note a normal radical extension field of $\mathbb{Q}$ exists by Theorem 102, page 201. We construct this normal radical extension field as follows.
By Definition 79, page 198, of a radical extension we know F is a splitting field over $\mathbb{Q}$ with elements $u_1, u_2, \ldots, u_m \in F$ such that,

1. $F = \mathbb{Q}(u_1, u_2, \ldots, u_m)$
2. $u^{n_1} \in \mathbb{Q}$ and $u_i^{n_i} \in \mathbb{Q}(u_1, u_2, \ldots, u_{i-1})$ for $n_i \in \mathbb{Z}$ for $1 \leq i \leq m$.

Let n be the least common multiple of the exponents n_i so that $n_i | n$ for all $i = 1, \ldots, m$.
By adjoining a primitive n^{th} root of unity ζ we obtain a normal radical extension $F(\zeta)$ of $\mathbb{Q}$, that is, every irreducible polynomial in $\mathbb{Q}[x]$ that contains a root in $F(\zeta)$ is a product of linear factors in $F(\zeta)$.
This is true since successive powers of a primitive n^{th} root of unity generate all the

m^{th} roots of unity for any $m|n$ so[3] $F(\zeta)$ contains all the primitive n_i^{th} roots of unity ω_i for all i and therefore elements of the form $\sqrt[n_i]{u_i}(\omega_i)^k$, $k = 0, \ldots, n_i - 1$.

***

Therefore[4] by the Fundamental Theorem 98, (5), page 184, since $F(\zeta)$ is a normal extension of E we have for the corresponding groups that $Gal(F(\zeta)/E) \lhd Gal(F(\zeta)/\mathbb{Q})$. Further, by Theorem 95, (1) $\Leftrightarrow$ (3), page 181, since E is a splitting field over $\mathbb{Q}$ means E is also a normal extension of $\mathbb{Q}$ then again by the Fundamental Theorem we also have $Gal(E/\mathbb{Q}) \lhd Gal(F(\zeta)/E)$. We have the tower of fields,

---

[3]For example, a primitive $6th$ root of unity is $e^{\frac{2\pi i}{6}5}$ since $gcd(5,6) = 1$ and it generates all the 2^{nd} (± 1) and 3^{rd} roots of unity as follows:

$$\begin{aligned}
2^{nd}: \left(e^{\frac{2\pi i}{6}5}\right)^3 &= (e^{\pi i})^5 = -1;\\
\left(e^{\frac{2\pi i}{6}5}\right)^5 &= (e^{2\pi i})^4(e^{2\pi i}) = +1;\\
3^{rd}: \left(e^{\frac{2\pi i}{6}5}\right)^2 &= \left(e^{\frac{2\pi i}{3}3}\right)\left(e^{\frac{2\pi i}{3}2}\right) = e^{\frac{4\pi i}{3}};\\
\left(e^{\frac{2\pi i}{6}5}\right)^4 &= e^{\frac{2\pi i}{3}10} = \left(e^{\frac{2\pi i}{3}3}\right)^3\left(e^{\frac{2\pi i}{3}}\right) = e^{\frac{2\pi i}{3}}
\end{aligned}$$

[4]We will be using the Fundamental Theorem 98 several times, specifically part (5). We proved, Let F be the splitting field of a separable polynomial over the field K and $G = Gal(F/K)$. Then we have the series of groups and fields,

$$\begin{aligned}
&G > G_1 > G_2 > \ldots > G_i > \ldots > \{e\}\\
&F > F_1 > F_2 > \ldots > F_j > \ldots > K, \ where,
\end{aligned}$$

1) For H a subgroup of G, the corresponding subfield is F^H and $H = Gal(F/F^H)$.

2) If F^H is a subfield of F containing K, the corresponding subgroup of G is $Gal(F/F^H) = H$.

3) There is a one-to-one reversing correspondence between the subgroups of G and the subfields of F that contain K.

4) For any subgroup H of G,

$$\begin{aligned}
[F : F^H] &= |H|, \text{ and,}\\
[F^H : K] &= [G : H]
\end{aligned}$$

5) The subgroup H is normal if and only if the subfield F^H is a normal extension of K and in this case,

$$Gal(F^H/K) \cong Gal(F/K)/Gal(F/F^H)$$

$$\begin{array}{c} F(\zeta) \\ | \\ E \\ | \\ \mathbb{Q} \end{array}$$

and the chain of subgroups,

$$Gal(E/\mathbb{Q}) \lhd Gal(F(\zeta)/E) \lhd Gal(F(\zeta)/\mathbb{Q})$$

satisfying the conditions of the Fundamental Theorem 98 (5), page 184, of Galois Theory. Hence,

$$Gal(E/\mathbb{Q}) \cong Gal(F(\zeta)/\mathbb{Q})/Gal(F(\zeta)/E)$$

or in other words, $Gal(E/\mathbb{Q})$ is isomorphic to the factor group of $Gal(F(\zeta)/\mathbb{Q})$ determined by $Gal(F(\zeta)/E)$.

*****

Next we show $Gal(F(\zeta)/\mathbb{Q})$ is solvable. Let $\mathbb{Q}(\zeta, u_1, \ldots, u_i) = F_i$. Since F_{i-1} contains all the n_i^{th} roots of unity, F_i is the splitting field of $x^{n_i} - a_i$ for some $a_i \in F_{i-1}$. We have developed, in the usual inverse sense, the corresponding towers of fields and groups as shown below. The minimal polynomials that are of the form $x^{n_i} - a_i$, are shown for three of the linkages and the minimal polynomial $x^n - 1$ applying to the first linkage.

$$\begin{array}{c} \mathbb{Q}(\zeta, u_1, u_2, \ldots, u_m) \\ | \\ \vdots \\ | \\ \mathbb{Q}(\zeta, u_1, u_2, \ldots, u_i) = F_i \\ p_i(x) = x^{n_i} - u_i \mid \\ \mathbb{Q}(\zeta, u_1, u_2, \ldots, u_{i-1}) = F_{i-1} \\ | \\ \vdots \\ | \\ \mathbb{Q}(\zeta, u_1, u_2) = F_2 \\ | \\ \mathbb{Q}(\zeta, u_1) = F_1 \\ p_1(x) = x^{n_1} - u_2 \mid \\ \mathbb{Q}(\zeta) \\ p_0(x) = x^n - 1 \mid \\ \mathbb{Q} \end{array}$$

Tower of subfields

$$\begin{array}{c} Gal(F(\zeta)/F_m) = \{e\} \\ | \\ \vdots \\ | \\ Gal(F(\zeta)/F_i) \\ | \\ Gal(F(\zeta)/F_{i-1}) \\ | \\ \vdots \\ | \\ Gal(F(\zeta)/F_2) \\ | \\ Gal(F(\zeta)/F_1) \\ | \\ Gal(F(\zeta)/\mathbb{Q}(\zeta)) \\ | \\ Gal(F(\zeta)/\mathbb{Q}) \end{array}$$

Tower of Subgroups

Now F_{i-1} contains all the n_i^{th} roots of unity, so F_i is the splitting field of $x^{n_i} - a_i$ for some $a_i \in F_{i-1}$. Therefore by Theorem 95, (1) $\Leftrightarrow$ (3), page 181, F_i is a normal extension of F_{i-1} and and therefore by the Fundamental Theorem 98 (5), page 184, the Galois group $Gal(F(\zeta)/F_i)$ is a normal subgroup of $Gal(F(\zeta)/F_{i-1})$ and,

$$Gal(F_i/F_{i-1}) \cong Gal(F(\zeta)/F_{i-1})/Gal(F(\zeta)/F_i) \tag{13.2.4}$$

But also by Theorem 101, page 199, $Gal(F_i/F_{i-1})$ is cyclic so that, by Theorem 4, page 33, it is also abelian. Therefore by (13.2.4) the isomorphic factor groups $Gal(F(\zeta)/F_{i-1})/Gal(F(\zeta)/F_i)$ are also abelian.
By the same argument $Gal(F(\zeta)/\mathbb{Q}))$ is normal in $Gal(F/\mathbb{Q})$ since $F(\zeta)$ is the splitting field of the minimal polynomial of ζ which is $x^n - 1$. Hence,

$$Gal(F(\zeta)/\mathbb{Q})/Gal(F(\zeta)/\mathbb{Q}(\zeta)) \cong Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$$

which is abelian by Theorem 100 on page 199.

The descending chain of normal subgroups,

$$Gal(F(\zeta)/\mathbb{Q}) \supseteq Gal(F(\zeta)/\mathbb{Q}(\zeta)) \supseteq Gal(F(\zeta)/\mathbb{Q}(\zeta, u_1)) \supseteq \\ \ldots \supseteq Gal(F(\zeta)/\mathbb{Q}(\zeta, u_1, \ldots, u_m)) = \{e\}$$

with each factor group abelian, shows that $Gal(F(\zeta)/\mathbb{Q})$ is a solvable group.

*****

Finally, by the Fundamental Theorem 98, page 184, of Galois Theory, $Gal(F(\zeta)/E)$ is a normal subgroup of $Gal(F(\zeta)/\mathbb{Q})$.
Hence the factor group $Gal(F(\zeta)/\mathbb{Q})/Gal(F(\zeta)/E)$ is solvable by Theorem 42, page 85.
But then, using (13.2.3), the isomorphic group $Gal(E/\mathbb{Q})$ is solvable, concluding the proof of the theorem. □

Note 26. *The conditions of the Fundamental Theorem of Galois Theory require the extension field F to be the splitting field of a separable polynomial over a base field K. This means whenever we use this theorem we are assuming any related $f(x)$ is separable or has no repeated roots. This requirement also follows from Theorems 88, 91 and 95 as well as Corollary 89, all of which lead on to the Fundamental Theorem.*

13.3 Insolvable Quintic Equations

We are ready to conclude. Theorem 39, page 81, proved S_n is not solvable for $n \geq 5$ so we only need to find a polynomial of degree ≥ 5 whose Galois group is (isomorphic to) S_n. We will apply the contrapositive statement of Theorem 104, namely, if the Galois group of $f(x)$ over $\mathbb{Q}$ is not solvable, then the equation $f(x) = 0$ is not solvable

by radicals.
So let's find an actual polynomial that is not solvable by radicals. We need the following two theorems.

Theorem 105. ***** (Cauchy - this version due to Pinter)*
Let G be a finite group of order n and let p be a prime divisor of n. Then G has an element of order p and subsequently a subgroup of order p.

Proof. Let G be a finite group of order n and let p be a prime divisor of n.
Consider all the p–tuples $(a_1, a_2, \ldots, a_{p-1}, a_p)$ of elements of G whose product $a_1 a_2, \cdots a_{p-1} a_p = e$.
If we select the $p-1$ elements $(a_1, a_2, \ldots, a_{p-1})$ at random, and note a group contains the inverse of each element, then there is a unique a_p such that $a_p = a_{p-1}^{-1} a_{p-2}^{-1} \cdots a_2^{-1} a_1^{-1}$, making,

$$a_1 a_2 \cdots a_{p-2} a_{p-1} a_{p-1}^{-1} a_{p-2}^{-1} \cdots a_2^{-1} a_1^{-1} = e.$$

Noting they are not necessarily all distinct, given G has order n, there are n choices for each of the $p-1$ elements of $a_p = a_{p-1}^{-1} a_{p-2}^{-1} \cdots a_2^{-1} a_1^{-1}$, and therefore we can obtain n^{p-1} tuples.
We call two p–tuples equivalent if one is merely a cyclic permutation of the other. Thus $(a_1, a_2, \ldots, a_{p-1}, a_p)$ is equivalent to exactly p distinct tuples, namely[5],

$$(a_1, a_2, \ldots, a_{p-1}, a_p),\ (a_2, a_3, \ldots, a_{p-1}, a_p, a_1),\ (a_3, a_4, \ldots, a_{p-1}, a_p, a_1, a_2),$$
$$\ldots,\ (a_p, a_1, \ldots, a_{p-2}, a_{p-1})$$

But we cannot say p divides n^{p-1} since, provided[6] p is a prime, a p–tuple of the form $(a, a, \ldots, a)$ with $a.a.\cdots.a = e$ is equivalent only to itself.
In order to prove the theorem we assume there are no p–tuples of the form $(a, a, \ldots, a)$ other than obviously $(e, e, \ldots, e)$. Removing $(e, e, \ldots, e)$, under this assumption there are p equivalence classes for each $(a_1, a_2, \ldots, a_p)$ in the remaining total of $n^{p-1} - 1$ p–tuples.
Hence,

$$p \mid n^{p-1} - 1 \Rightarrow n^{p-1} \equiv 1 (\mathrm{mod} p)$$

But in the statement of the theorem we have

$$p \mid n \Rightarrow p \mid n^{p-1} \Rightarrow n^{p-1} \equiv 0 (\mathrm{mod} p).$$

[5]You can imagine this as the elements $(a_1, a_2, \ldots, a_p)$ placed on a "clock with p hours" with a_1 in the "12" position and so on all the way around to a_p in the "11" position. Then rotate the clock clockwise for one "hour" to obtain the first cyclic permutation and so on.

[6]If p is not a prime, say $p = jk$, then tuples of the form $(a, a, \ldots, a, b, a, a, \ldots, a, b)$ where $(a, a, \ldots, a, b)$ has length j (or k) will not yield p equivalence classes, since rotating the "clock" will result in the same form after just j rotations of one "hour".

This contradiction proves there must be a p–tuple of the form $(a, a, \ldots, a)$ with $a.a.\cdots a = a^p = e$, that is, there is an element $a \in G$ of order p.
Finally, the cyclic group $< a >$ is a subgroup of G of order p since if $a \in G$ then so does every power of a and if p is prime then the only powers of a that survive are $a, a^2, \ldots, a^p = 1$ which is the definition of the cyclic group $< a >$. □

Note 27. *Let us review the relationship between S_n and the $Gal(F/K)$ where F is the splitting field of a polynomial $f(x) \in K[x]$ of degree n.*
The $Gal(F/K)$ is the set of automorphisms that, by Theorem 86, page 162, permute the roots of $f(x)$, degree n, and $|Gal(F/K)| \leq n!$, by Corollary 89, page 166 and Theorem 84, page 158.
S_n is the set of automorphisms from $\{1, 2, \ldots, n\}$ to $\{1, 2, \ldots, n\}$ that, by definition, permute the set $\{1, 2, \ldots, n\}$ and, by Theorem 7, page 40, $|S_n| = n!$
Accordingly, if we label the roots of $f(x)$ as $\{1, 2, \ldots, n\}$ we can regard $Gal(F/K)$ as a subgroup of S_n.

Theorem 106. *****
Let $f(x) \in \mathbb{Q}[x]$ be an irreducible quintic[7] having exactly three real zeros. Then $f(x)$ is not solvable by radicals over $\mathbb{Q}$.

Proof. Let $F \subseteq \mathbb{C}$ be the splitting field of a polynomial $f(x)$ over $\mathbb{Q}$ and let u_1, u_2, u_3 be the three real zeros. Then the other two[8] zeros u_4, u_5 must be complex conjugates of each other. This is so, since given the three real zeros, $f(x)$ must factor as,

$$f(x) = (x - u_1)(x - u_2)(x - u_3)(ax^2 + bx + c)$$

and by the quadratic formula, the roots of $(ax^2 + bx + c)$ are $x = \dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ so when $b^2 - 4ac < 0$ the roots are complex conjugates are complex conjugates, say $c \pm di$.
So we have the roots $\{u_1, u_2, u_3, c + di, c - di\}$.
The Galois group of $F/\mathbb{Q}$ consists of automorphisms which permute these roots. We have already met complex conjugation which interchanges complex conjugates thus,

$$\phi : c + di \to c - di$$
$$\phi : c - di \to c + di$$

And we noted ϕ does not change $u_1, u_2, u_3 \in \mathbb{R}$ which can be written as,

$$\phi : u \pm 0i \to u \mp 0i$$

So, since complex conjugation is an automorphism fixing the base field $\mathbb{Q}$, then its restriction to F is an element of $Gal(F/\mathbb{Q})$.

[7] By Note 26, page 207, this $f(x)$ must be separable or have no multiple roots.
[8] Note by Corollary 50, page 99, a degree 5 polynomial cannot have more than 5 roots, so if it is separable then it has exactly 5 roots.

So, when $Gal(F/\mathbb{Q})$ is viewed as a subgroup of S_5, ϕ will be precisely the 2-cycle $(4,5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix}$ which interchanges the two complex roots 4 and 5 according to,

$$\phi(c+di) = c-di,\ \phi(c-di) = c+di$$

Also, since $f(x)$ is irreducible by assumption and has degree 5, then $[F:\mathbb{Q}] = 5$ and so $|Gal(F/\mathbb{Q})| = [F:\mathbb{Q}]$ is divisible by 5.
Hence by Cauchy's Theorem 105 above, $Gal(F/\mathbb{Q})$ has an element of order 5.
Again, viewing $Gal(F/\mathbb{Q})$ as a subgroup of S_5, then $Gal(F/\mathbb{Q})$ has an element of order 5. But the elements of S_5 of order 5 are precisely the 5-cycles.
Therefore $Gal(F/\mathbb{Q})$, viewed as a subgroup of S_5, contains both a 2-cycle and a 5-cycle. Then[9] by Theorem 14, $Gal(F/\mathbb{Q}) = S_5$ which, by Theorem 40, page 83, is not a solvable group.
We conclude, by Theorem 104, page 204, this irreducible quintic $f(x) \in \mathbb{Q}$ is not solvable by radicals. □

Now let's find a specific quintic polynomial not solvable by radicals. There are many of them and various algebra textbooks quote different ones but they all mostly use the same method of proof, namely, they show their particular polynomial is irreducible (by applying the Eisenstein criterion) and that the polynomial has exactly three real roots (by using differential calculus). Per Note 26, page 207, we must show our $f(x)$ is separable or has no multiple roots. The conclusion of insolvability follows from Theorem 106.

Example 99. *$f(x) = x^5 - 4x + 2$ is not solvable by radicals.*
Proof: Note, if $f(x) = x^5 - 4x + 2 = a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ then $a_5 = 1, a_4 = 0, a_3 = 0, a_2 = 0, a_1 = -4, a_0 = 2$.
Then $f(x) = x^5 - 4x + 2$ is irreducible by Eisenstein's criterion[10] since the prime 2 divides $a_0 = 2$ and also divides $a_4 = a_3 = a_2 = 0$ but $2^2 \nmid a_0$ and $2 | a_1 = -4$ but $2 \nmid a_5 = 1$.
(OK, we need differential Calculus or just study the graph below.)
Next, according to Note 26, page 207 we need to show this $f(x)$ is separable. We use Theorem 90, page 172 to show $gcd(f(x), f'(x)) = 1$.
Now $f(x) = x^5 - 4x + 2 \Rightarrow f'(x) = 5x^4 - 4$. The roots of $5x^4 - 4 = 0$ are given by,

$$f'(x) = 5x^4 - 4 = 0 \Rightarrow x^2 = \sqrt{\frac{4}{5}} \text{ or } x^2 = -\sqrt{\frac{4}{5}} \Rightarrow x = \pm\sqrt[4]{\frac{4}{5}},$$

and when substituted into $f(x)$ none of them yield a value of 0.
Hence $gcd(f(x), f'(x)) = 1$ so $f(x)$ has no multiple roots.

[9] Theorem 14, page 50, proved that every element in S_5 can be written as the product of powers of $(1,2,3,4,5)$ and $(1,2)$, that is the cycles $(1,2,3,4,5)$ and $(1,2)$ generate S_5.

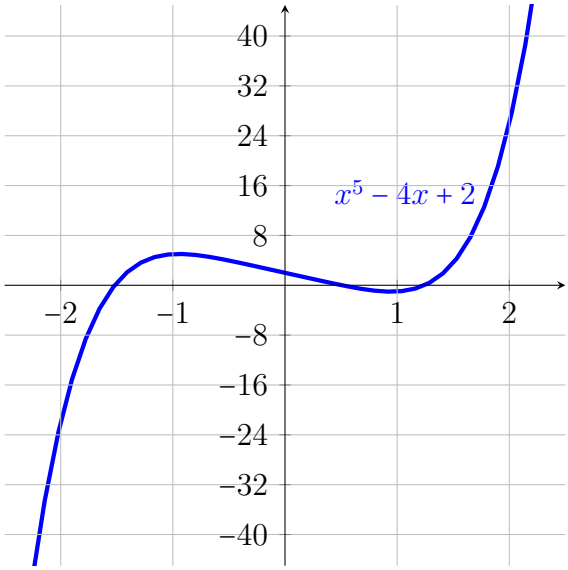
[10] Eisenstein's criterion, Theorem 70B, 125, for factoring $f(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$, $a_n > 0$, $a_i \in \mathbb{Z}$ is that if there is a prime p that may divide a_0 but $p^2 \nmid a_0$ and which divides all the other coefficients except a_n, then $f(x)$ is irreducible over $\mathbb{Q}$.

Let us proceed to show $f(x)$ *has three real roots and two complex ones. We use differential calculus again.*
Since $f''(x) = 20x^3$ *there is a maximum point at* $\left(-\sqrt[4]{\frac{4}{5}} \approx -0.95, f\left(-\sqrt[4]{\frac{4}{5}}\right) \approx 5\right)$ *and a minimum point at* $\left(\sqrt[4]{\frac{4}{5}} \approx 0.95, f\left(\sqrt[4]{\frac{4}{5}}\right) \approx -1\right)$.

These two critical points, combined with the observations that,

$$\begin{aligned} f(x > 2) &= x(x^4 - 4) + 2|_{x>2} > 26, \\ f(2) = 26, f(1) &= -1, f(0) = 2, f(-1) = 5, f(-2) = -22, \\ f(x < -2) &= x(x^4 - 4) + 2|_{x<-2} < -22 \end{aligned}$$

show $f(x)$ *has exactly three real roots since the graph crosses the* $x-$*axis exactly three times, specifically between 1 and 2, 0 and 1 and -1 and -2. See the graph below. Hence, by Theorem 106,* $f(x) = x^5 - 4x + 2$ *is insolvable by radicals.*



◇

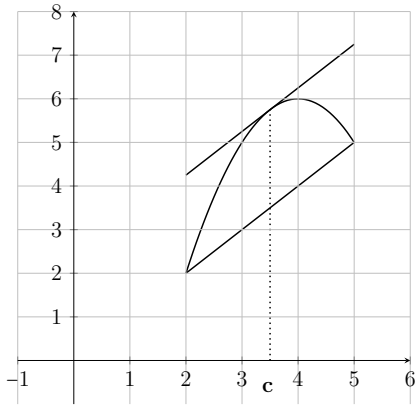
Appendix A

Taylor Series and Roots of Unity

In this appendix we assume the reader has studied differential calculus for at least one semester.

A.1 Mean Value Theorem

The mean value theorem of Calculus states that if a line segment is drawn joining the end points of a smooth curve then there is at least one point $(c, f(c))$ on the curve where the tangent at that point and the line segment are parallel or have the same slope. The diagram below illustrates the theorem. If the line segment has a slope of zero then there are an infinite number of such points with $x-$coordinate c. Otherwise, the number of c points depends upon the number of maximum and minimum points between the two end points.



Let us now consider a general theorem that can be used to express "nice" or smooth functions as a polynomial-type infinite series called, after their discoverer, Taylor Series.

A.2 Taylor Series

Definition 81. *smooth function*
A smooth function at a point is a function that can be differentiated an infinite number of times at that point.

Theorem 107. ***
Suppose a smooth function has the representation $f(x) = c_0 + c_1x + c_2x^2 + \ldots$ *for all values of* x *near* 0*. Then,*

$$c_n = \frac{f^{(n)}(0)}{n!}, \ for\ all\ n \in \mathbb{Z}^+ \cup \{0\}$$

Proof.

$$\begin{aligned}
f(x) &= c_0 + c_1x + c_2x^2 + c_3x^3 + c_4x^4 + \ldots + c_nx^n + \ldots \\
f'(x) &= 1!c_1 + 2c_2x + 3c_3x^2 + 4c_4x^3 + \ldots + nc_nx^{n-1} + \ldots \\
f''(x) &= 2!c_2 + 3\cdot 2c_3x + 4\cdot 3c_4x^2 + \ldots + n(n-1)x^{n-2} + \ldots \\
f'''(x) &= 3!c_3 + 4\cdot 3\cdot 2c_4x + \ldots + n(n-1)(n-2)c_nx^{n-3} + \ldots \\
&\vdots
\end{aligned}$$

Substituting $x = 0$ into these equations yields,

$$c_0 = f(0),\ c_1 = \frac{f'(0)}{1!},\ c_2 = \frac{f''(0)}{2!},\ c_3 = \frac{f'''(0)}{3!},\ c_4 = \frac{f^{(4)}(0)}{4!}, \ldots \Rightarrow c_n = \frac{f^{(n)}(0)}{n!}$$

□

Theorem 108. ***
Suppose a function is smooth for all points in an interval about $x = 0$*. Then for all* x *in that interval, we can write,*

$$f(x) = f(0) + \frac{f'(0)}{1!}x + \frac{f''(0)}{2!}x^2 + \frac{f'''(0)}{3!}x^3 + \ldots + \frac{f^{(n)}(0)}{n!}x^n + R_n(x),$$

where the remainder $R_n(x) = \dfrac{f^{(n+1)}(c)}{(n+1)!}x^{n+1}$ *and* c *is some point between* x *and* 0*.*

Proof. Define,

$$R_n(x) = f(x) - f(0) - \frac{f'(0)}{1!}x - \frac{f''(0)}{2!}x^2 - \frac{f'''(0)}{3!}x^3 - \ldots - \frac{f^{(n)}(0)}{n!}x^n$$

Define,

$$\begin{aligned}
g(t) = f(x) - f(t) - \frac{f'(t)}{1!}(x-t) - \frac{f''(t)}{2!}(x-t)^2 - \frac{f'''(t)}{3!}(x-t)^3 \\
- \ldots - \frac{f^{(n)}(t)}{n!}(x-t)^n - R_n(x)\frac{(x-t)^{n+1}}{x^{n+1}}
\end{aligned}$$

where we regard x as a constant. Then,

$$g(x) = f(x) - f(x) - \frac{f'(x)}{1!}(x-x) - \frac{f''(x)}{2!}(x-x)^2 - \frac{f'''(x)}{3!}(x-x)^3 - \ldots - \frac{f^{(n)}(x)}{n!}(x-x)^n - R_n(x)\frac{(x-x)^{n+1}}{x^{n+1}} = 0$$

and,

$$g(0) = f(x) - f(0) - \frac{f'(0)}{1!}x - \frac{f''()x)}{2!}x^2 - \frac{f'''(0)}{3!}x^3 - \ldots - \frac{f^{(n)}(0)}{n!}x^n - R_n(x)\frac{x^{n+1}}{x^{n+1}} = R_n(x) - R_n(x) = 0$$

Since $g(x) = g(0) = 0$, making the slope of the line segment joining them equal to 0, by the Mean Value Theorem[1] there is a point on the curve with x–coordinate c such that $g'(c) = 0$. Now, using the product and chain rules,

$$\begin{aligned} g'(t) &= 0 - \cancel{f'(t)} - \cancel{\frac{f''(t)}{1!}(x-t)} + \cancel{\frac{f'(t)}{1!}} - \cancel{\frac{f'''(t)}{2!}(x-t)^2} + \cancel{\frac{f''(t)}{1!}(x-t)} - \ldots \\ &\quad - \frac{f^{n+1}(t)}{n!}(x-t)^n + \cancel{\frac{f^{n+1}(t)}{(n-1)!}(x-t)^{n-1}} + R_n(x)\frac{(n+1)(x-t)^n}{x^{n+1}} \\ &= -\frac{f^{n+1}(t)}{n!}(x-t)^n + R_n(x)\frac{(n+1)(x-t)^n}{x^{n+1}} \end{aligned}$$

Then, substituting $x = c$,

$$\begin{aligned} 0 = g'(c) &= -\frac{f^{(n+1)}(c)}{n!}(x-c)^n + R_n(x)\frac{(n+1)(x-c)^n}{x^{n+1}} \\ \Rightarrow R_n(x)\frac{(n+1)(x-c)^n}{x^{n+1}} &= \frac{f^{(n+1)}(c)}{n!}(x-c)^n \\ \Rightarrow R_n(x) &= \frac{f^{(n+1)}(c)}{(n+1)n!}x^{n+1} \\ \Rightarrow R_n(x) &= \frac{f^{(n+1)}(c)}{(n+1)!}x^{n+1} \end{aligned}$$

□

[1]The mean value theorem states that for any continous curve $g(x)$ joining two points A, B with x–coordinates $x = a, x = b$ there is a point $(c, g(c))$ on the curve such that $a \le c \le b$ and the slope of the curve at this point, $(c, g(c))$, is the same as the slope of the line segment joining A and B, that is, $g'(c) = \dfrac{g(b) - g(a)}{b - a}$.

Theorem 109. *** (Taylor's Theorem)*
Let $f(x)$ be a smooth function for all points in an interval $(-r, r)$ about 0. The Taylor series defined by

$$f(0) + \frac{f'(0)}{1!}x + \frac{f''(0)}{2!}x^2 + \frac{f'''(0)}{3!}x^3 + \ldots + \frac{f^{(n)}(0)}{n!}x^n + \ldots,$$

converges to $f(x)$ on the interval $(-r, r)$ as $n \to \infty$ if and only if,

$$\lim_{n\to\infty} R_n(x) = 0 \text{ where } R_n(x) = \frac{f^{(n+1)}(c)}{(n+1)!}x^{n+1}$$

and c is some point between x and 0.
That is, we have

$$f(x) = f(0) + \frac{f'(0)}{1!}x + \frac{f''(0)}{2!}x^2 + \frac{f'''(0)}{3!}x^3 + \ldots + \frac{f^{(n)}(0)}{n!}x^n + \ldots,$$

for any point x in $(-r, r)$ if and only if,

$$\lim_{n\to\infty} \frac{f^{(n+1)}(c)}{(n+1)!}x^{n+1} = 0$$

for some point c between x and 0.

Proof. Assume

$$\lim_{n\to\infty} R_n(x) = \lim_{x\to\infty} \frac{f^{(n+1)}(c)}{(n+1)!}x^{n+1} = 0$$

We want to show that

$$f(0) + \frac{f'(0)}{1!}x + \frac{f''(0)}{2!}x^2 + \frac{f'''(0)}{3!}x^3 + \ldots + \frac{f^{(n)}(0)}{n!}x^n + \ldots,$$

converges to $f(x)$ as $n \to \infty$. Let,

$$p_n(x) = f(0) + \frac{f'(0)}{1!}x + \frac{f''(0)}{2!}x^2 + \frac{f'''(0)}{3!}x^3 + \ldots + \frac{f^{(n)}(0)}{n!}x^n$$

Note the Taylor series is $\lim_{n\to\infty} p_n(x)$. Then, using the result of Theorem 108 above,

$$p_n(x) = f(x) - R_n(x) \Rightarrow \lim_{n\to\infty} p_n(x) = \lim_{n\to\infty} f(x) - \lim_{n\to\infty} R_n(x) = f(x) - 0$$

$$\Rightarrow f(x) = \lim_{n\to\infty} p_n(x) = f(0) + \frac{f'(0)}{1!}x + \frac{f''(0)}{2!}x^2 + \frac{f'''(0)}{3!}x^3 + \ldots + \frac{f^{(n)}(0)}{n!}x^n + \ldots$$

Conversely, assume the Taylor series converges to $f(x)$ on $(-r, r)$, that is,

$$f(x) = \lim_{x\to\infty} p_n(x).$$

Then,

$$0 = f(x) - \lim_{n\to\infty} p_n(x) = \lim_{n\to\infty} (f(x) - p_n(x)) = \lim_{n\to\infty} R_n(x)$$

□

A.3 Taylor Series of the Exponential Function

Theorem 110. ** *The Taylor series for the natural exponential function is,*

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots + \frac{x^n}{n!} + \ldots = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

Proof. Let $f(x) = e^x$. Then the n^{th} derivative $f^{(n)}(x) = e^x$ for all n and $f^{(n)}(0) = e^0 = 1$ for all n. Then the general Taylor series,

$$f(x) = f(0) + \frac{f'(0)}{1!}x + \frac{f''(0)}{2!}x^2 + \frac{f'''(0)}{3!}x^3 + \ldots + \frac{f^{(n)}(0)}{n!}x^n + \ldots,$$

gives,

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots + \frac{x^n}{n!} + \ldots = \sum_{n=0}^{\infty} \frac{x^n}{n!},$$

since,

$$\lim_{n\to\infty} R_n(x) = \lim_{n\to\infty} \frac{f^{n+1}(c)}{(n+1)!}x^{n+1} = \lim_{n\to\infty} \frac{e^c}{(n+1)!}x^{n+1} = 0$$

since the denominator is approaching infinity much more rapidly that the numerator. □

A.4 Taylor Series for Sine and Cosine Functions

Theorem 111. ** *For all values of x,*

$$\sin x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \ldots = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^{2n-1}}{(2n-1)!}$$
$$\cos x = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \ldots = \sum_{n=0}^{\infty} (-1)^{n} \frac{x^{2n}}{(2n)!}$$

Proof. Let,

$$\begin{aligned} & f(x) = \sin x \\ & \Rightarrow f'(x) = \cos x \\ & \Rightarrow f''(x) = -\sin x \\ & \Rightarrow f'''(x) = -\cos x \\ & \Rightarrow f^{(4)}(x) = \sin x \end{aligned}$$

Clearly this pattern repeats every four derivatives. Then we have these four terms repeated,

$$f(0) = 0,\ f'(0) = 1,\ f''(0) = 0,\ f'''(0) = -1.$$

Thus,

$$f(x) = f(0) + \frac{f'(0)}{1!}x + \frac{f''(0)}{2!}x^2 + \frac{f'''(0)}{3!}x^3 + \ldots + \frac{f^{(n)}(0)}{n!}x^n + \ldots,$$

gives

$$\sin x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \ldots = \sum_{n=1}^{\infty}(-1)^{n+1}\frac{x^{2n-1}}{(2n-1)!}$$

provided $\lim_{n\to\infty} R_n = \lim_{n\to\infty} \frac{f^{(n+1)}(c)}{(n+1)!} = 0$. But $f^{(n+1)}(c)$ is one of $\pm\sin c, \pm\cos c$ which take values between -1 and $+1$. So we have,

$$-1 \le f^{(n)}(c) \le +1 \Rightarrow -\frac{x^{(n+1)}}{(n+1)!} \le f^{(n)}(c)\frac{x^{(n+1)}}{(n+1)!} \le \frac{x^{(n+1)}}{(n+1)!}$$

Now both of $\lim_{n\to\infty} \pm \frac{x^{(n+1)}}{(n+1)!} = 0$ since[2] $(n+1)! \to \infty$ much much more rapidly than does the numerator $x^{(n+1)}$.
Hence,

$$\lim_{n\to\infty} R_n = \lim_{n\to\infty} \frac{f^{(n+1)}(c)}{(n+1)!} = 0.$$

We could repeat this argument for $\cos x$ but it is easier to use $\frac{d\sin x}{dx} = \cos x$. So, if we differentiate $\sin x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \ldots$ with respect to x, we obtain,

$$\cos x = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \ldots = \sum_{n=0}^{\infty}(-1)^n\frac{x^{2n}}{(2n)!}$$

□

A.5 Euler's Formulas

We reach two of the most famous and most useful formulas in the whole of mathematics. The second one is wonderful, combining two transcendental numbers with a complex number to produce an integer!

[2]Strictly speaking we should invoke the Squeeze Theorem, which says if at a given point a function is squeezed between two other functions both approaching the same limit at that point then it must also be approaching that same limit at that point.

Theorem 112. * *(Euler)*

$$e^{ix} = \cos x + i \sin x, \ \textit{where } i = \sqrt{-1}$$
$$e^{\pi i} = -1$$

Proof.

$$\begin{aligned}
e^x &= 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots + \frac{x^n}{n!} + \ldots \\
\Rightarrow e^{ix} &= 1 + ix + \frac{(ix)^2}{2!} + \frac{(ix)^3}{3!} + \frac{(ix)^4}{4!} + \frac{(ix)^5}{5!} + \frac{(ix)^6}{6!} + \frac{(ix)^7}{7!} + \frac{(ix)^8}{8!} + \ldots \\
&= 1 + ix - \frac{x^2}{2!} - i\frac{x^3}{3!} + \frac{x^4}{4!} + i\frac{x^5}{5!} - \frac{x^6}{6!} - i\frac{x^7}{7!} + \frac{x^8}{8!} + \ldots \\
&= 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \frac{x^8}{8!} + \ldots + i\big(x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \ldots\big) \\
&= \cos x + i \sin x
\end{aligned}$$

Put $x = \pi$, then,

$$e^{\pi i} = \cos \pi + i \sin \pi = -1 + i \cdot 0 = -1$$

□

Here are two examples of the usefulness of these results.

Corollary 113. *(De Moivre's Formula)*

$$(\cos x + i \sin x)^n = \cos nx + i \sin nx$$

Proof.

$$(\cos x + i \sin x)^n = (e^{ix})^n = e^{inx} = \cos nx + i \sin nx$$

□

Corollary 114. *Complex Formulas for* $\sin x$ *and* $\cos x$.

$$\sin x = \frac{e^{ix} - e^{-ix}}{2i}$$
$$\cos x = \frac{e^{ix} + e^{-ix}}{2}$$

Proof.

$$\begin{aligned}
e^{ix} &= \cos x + i \sin x \\
&\Rightarrow e^{-ix} = e^{i(-x)} = \cos(-x) + i \sin(-x) = \cos x - i \sin x
\end{aligned}$$

Add and subtract the two equations to obtain,

$$\sin x = \frac{e^{ix} - e^{-ix}}{2i}$$
$$\cos x = \frac{e^{ix} + e^{-ix}}{2}$$

□

A.6 Roots of Unity

Complex numbers are defined by $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}, i = \sqrt{-1}\}$.
Now the solution of $x^2 - 1 = 0 \Rightarrow x^2 = 1$ is $x = \pm 1$. We say ± 1 are the second roots of unity.
We can also solve, say, $x^4 - 1 = 0 \Rightarrow x^4 = 1$ by noting $(e^{\pi i})^4 = (-1)^4 = 1$ so that one solution is clearly $x = e^{\pi i}$.
However, since this is an equation of degree 4, we expect 4 solutions. They are,

$$x = e^{\frac{2k\pi i}{4}},\ k = 1, 2, 3, 4 \text{ or } x = e^{\frac{2\pi i}{4}},\ x = e^{\frac{4\pi i}{4}},\ x = e^{\frac{6\pi i}{4}},\ x = e^{\frac{8\pi i}{4}},$$

since,

$$x^4 = \left(e^{\frac{2k\pi i}{4}}\right)^4 = (e^{2k\pi i}) = (e^{\pi i})^{2k} = (-1)^{2k} = 1$$

The numbers $x = e^{\frac{2\pi i}{4}},\ x = e^{\frac{4\pi i}{4}},\ x = e^{\frac{6\pi i}{4}},\ x = e^{\frac{8\pi i}{4}}$, are called the 4th roots of unity.

Definition 82. *roots of unity*
The n^{th} roots of unity are the solutions of the equation $x^n = 1$. They are

$$e^{\frac{2k\pi i}{n}},\ 0 \le k \le (n-1).$$

Bibliography

[1] Beachey, J.A., and Blair, W.D. *Abstract Algebra,* 2nd ed., Waveland Press, Illinois, 1996

[2] Childs, L.N., *A Concrete Introduction to Higher Algebra,* 2nd ed., Springer-Verlag, N.Y., 1995

[3] Frahleigh, J.B., *A First Course in Abstract Algebra,* 3rd ed., Addison-Wesley, USA, 1982

[4] Hall, M., *The Theory of Groups,* Macmillan, NY, 1959

[5] Hungerford, T., *Algebra,* Springer-Verlag, GTM 73, NY, 1974

[6] Jacobsen, N., *Basic Algebra,* 2nd ed., W.H. Freeman and Co., San Francisco, 1985

[7] Lang, S., *Algebra.* 3rd ed., Addison-Wesley, NY, 1999

[8] Morand, P., *Field and Galois Theory.* Springer-Verlag, GTM 167, NY, 1996

[9] Papantonopoulou, A., *Algebra, Pure and Applied,* Prentice Hall, NJ, 2002

[10] Scott, W.R., *Group Theory,* Dover Press, NJ, 1987

Index