WON Series in Discrete Mathematics and Modern Algebra Volume 6

FROM GROUPS TO GALOIS

Amin Witno

These notes[1] have been prepared for the students at Philadelphia University (Jordan) who are taking the Math 342–442 series of Abstract Algebra. Topics in group theory are covered in the first thirteen chapters, followed by another thirteen chapters on rings and fields. The remaining chapters are an attempt to introduce Galois theory as an independent reading project. Outline notes are more like a revision. No student is expected to fully benefit from these notes unless they have regularly attended the lectures.

1 Groups

By a *binary operation* $\star$ on a set, we mean a function taking each ordered pair a, b to another element in the set which shall be denoted by $a \star b$. The word *ordered* used here implies that in general $a \star b \neq b \star a$.

Definition. A *group* G is a set together with a binary operation $\star$ on G which satisfies the following three axioms.

1) For every elements $a, b, c \in G$, we have $a \star (b \star c) = (a \star b) \star c$.

2) There exists $e \in G$ such that $a \star e = a = e \star a$ hold for every element $a \in G$.

3) For each element $a \in G$, there exists $b \in G$ satisfying $a \star b = e = b \star a$.

Remark. Condition (1) in other words says that the operation $\star$ is *associative*. An element e satisfying condition (2) is called an *identity element* of G. We shall soon see that a group has exactly one identity element. In (3) we call b an *inverse* of a in G. We shall also prove that every $a \in G$ has a unique inverse.

Example. We give several examples of what a group might look like.

1) The set of integers $\mathbb{Z}$ together with ordinary addition, which is known to be associative, is a group. The number $e = 0$ is an identity element of $\mathbb{Z}$ and the inverse of any integer a in this case is $-a$.

   Similarly also, under addition, the following sets each form a group: the rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, and the complex numbers $\mathbb{C}$. From now on we

[1] Copyrighted under a Creative Commons License

Last Revision: 13–03–2022

awitno@gmail.com

shall simply say *the group* $\mathbb{Z}$, refering to the group of integers under addition; and likewise with the groups $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$.

2) The set of nonzero rational numbers $\mathbb{Q}^*$ is a group under the usual multiplication. Its identity element is $e = 1$ and each nonzero rational number a/b has inverse b/a. So do we have the groups $\mathbb{R}^*$ and $\mathbb{C}^*$ of nonzero numbers, respectively real and complex, under multiplication. However, note that $\mathbb{Z}^*$, the set of nonzero integers, is not a group under multiplication because, for instance, 2 has no inverse in it. (Why?) Henceforth, the groups $\mathbb{Q}^*$, $\mathbb{R}^*$, and $\mathbb{C}^*$ are always understood to be the groups of nonzero rational, real, and complex numbers, respectively, under multiplication.

3) The set $\{0\}$ under addition is a group, where 0 is the identity and only element of G. Essentially this is the only kind of a group with one element, denoted by $G = \{e\}$, and it is called the *trivial group.*

4) We can have a group with two elements, $G = \{e, a\}$, where e is identity and where the binary operation is defined by $a \star a = e$. You can check that it does satisfy the three axioms of a group.

5) The set $M(2, \mathbb{R})$ of 2×2 matrices with real entries is a group under matrix addition. Can you identify the identity element and the inverse of $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(2, \mathbb{R})$?

   Similarly, the set $M(n, S)$ of $n \times n$ matrices over S under matrix addition forms a group, where S may be the set of integers, rationals, or complex numbers.

6) The set $GL(2, \mathbb{R})$ of 2×2 matrices with nonzero determinants is also a group under matrix multiplication. We know from linear algebra that matrix multiplication is associative. The identity element here is $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, and recall that having a nonzero determinant is equivalent to being invertible.

Definition. We call the binary operation $\star$ *commutative* if $a \star b = b \star a$ for all. In that case the group G is called *abelian.* The examples given above are all abelian groups, except the last one is non-abelian since matrix multiplication is not commutative.

Proposition 1.1. Let G be a group with a given binary operation.

1) There is exactly one identity element in G.

2) Each $a \in G$ has a unique inverse in G.

Proof. Suppose there were two identity elements, e and f. Then $e \star f = f$ since e is identity, while at the same time $e \star f = e$ as f is identity. Hence $e = f$. This proves (1). For (2) assume a had two inverses b and c. Then $a \star b = a \star c = e$. Operate both sides by b from the left and then apply associativity to get

$$\begin{aligned} b \star (a \star b) &= b \star (a \star c) \\ (b \star a) \star b &= (b \star a) \star c \\ e \star b &= e \star c \\ b &= c \end{aligned}$$

This shows that a can have only one inverse. ▽

Remark. Now it makes sense to speak of *the* identity element of a group, which is almost always denoted by e, and of *the* inverse of an element a, denoted by a^{-1}. Moreover, for convenience we shall write ab instead of $a \star b$, and in particular, let $a^2 = a \star a$. To avoid confusion, however, when the operation is actually addition, we prefer to write $a + b$ instead of ab, as well as $-a$ instead of a^{-1}. It is also clear that by associativity we may write the product abc or $a_1 a_2 a_3 \cdots a_n$ without the necessity of brackets.

Proposition 1.2. For any elements in a group, the following statements hold.

1) $(a^{-1})^{-1} = a$

2) $(ab)^{-1} = b^{-1}a^{-1}$

3) $ab = ac$ implies $b = c$

4) $ba = ca$ implies $b = c$

Proof. In class. ▽

Remark. Properties (3) and (4) above go by the name *left* and *right cancellation laws,* respectively. We should not assume that cancellation laws always apply unless we know that we are dealing with group elements. We have, for example,

$$\begin{pmatrix} 0 & 1 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 4 \\ 4 & 8 \end{pmatrix}$$

seemingly contradicting (4). Can you account for this false counter-example?

Theorem 1.3. If G and H are two groups, with their respective binary operations, then the set $G \times H = \{(g, h) \mid g \in G, h \in H\}$ is a group under the operation defined by $(g, h)(g', h') = (gg', hh')$. The name for this group is the *direct product* of G and H.

Proof. Exercise. ▽

Exercise 1. Complete this homework set before we continue to the next section.

1) Prove that G is a group under the given binary operation $\star$.

   a) $G = \{3n \mid n \in \mathbb{Z}\}$; $a \star b = a + b$ for all $a, b \in G$
   b) $G = \{2^n \in \mathbb{Q} \mid n \in \mathbb{Z}\}$; $a \star b = a \times b$ for all $a, b \in G$
   c) $G = \{A \in M(2, \mathbb{Z}) \mid \det A = \pm 1\}$; $A \star B = A \times B$ for all $A, B \in G$
   d) $G = \{x \in \mathbb{R} \mid x \neq -1\}$; $a \star b = a + b + ab$ for all $a, b \in G$

2) Prove that “the mixed cancellation law” $ab = ca \to b = c$ for all $a, b, c \in G$ holds if and only if the group G is abelian.
3) Prove that a group G is abelian if and only if $(ab)^2 = a^2b^2$ for all $a, b \in G$.
4) Let G be a group. Prove that if $a^2 = e$ for all $a \in G$, then G is abelian.

2 The Group $\mathbb{Z}_n$

This section is devoted to the presentation of a group with a finite number of elements and which is called the modular integers. We assume a knowledge from set theory concerning an equivalence relation and its equivalence classes.

Definition. Fix an integer $n > 0$. Define two integers a, b to be *congruent mod* n when $a - b = nk$ for some integer k. We denote this relation by $a \equiv b \,(\operatorname{mod} n)$ and show that it is an equivalence relation over $\mathbb{Z}$:

1) *reflexive*: $a \equiv a \,(\operatorname{mod} n)$ since $a - a = nk$ with $k = 0$.

2) *symmetric*: $a \equiv b \,(\operatorname{mod} n)$ implies $b \equiv a \,(\operatorname{mod} n)$ because $a - b = nk$ implies $b - a = nh$ with $h = -k$.

3) *transitive*: $a \equiv b \,(\operatorname{mod} n)$ and $b \equiv c \,(\operatorname{mod} n)$ imply $a \equiv c \,(\operatorname{mod} n)$ because $a - b = nk$ and $b - c = nh$ imply $a - c = a - b + b - c = nj$ with $j = k + h$.

Now let the equivalence classes under this relation be called *congruence classes*, where for each $a \in \mathbb{Z}$ we denote its congruence class by

$$\begin{aligned} [a]_n &= \{b \in \mathbb{Z} \mid b \equiv a \,(\operatorname{mod} n)\} \\ &= \{b \in \mathbb{Z} \mid b - a = nk\} \\ &= \{nk + a \mid k \in \mathbb{Z}\} \end{aligned}$$

The following results follow from the fact about equivalence classes.

1) $a \in [a]_n$ for each $a \in \mathbb{Z}$, and $b \in [a]_n$ if and only if $a \equiv b \,(\operatorname{mod} n)$.

2) $[a]_n = [b]_n$ if and only if $a \equiv b \,(\operatorname{mod} n)$.

3) $[a]_n \cap [b]_n = \phi$ if and only if $a \not\equiv b \ (\operatorname{mod} n)$.

4) $\bigcup\{\, [a]_n \mid a \in \mathbb{Z}\} = \mathbb{Z}$.

It also means that each integer belongs to exactly one congruence class, i.e., the congruence classes partition the set $\mathbb{Z}$. Now we will be interested in knowing how many distinct congruence classes we have. For that we assume the following principle, called the *Division Algorithm*.

Theorem 2.1 (The Division Algorithm in $\mathbb{Z}$)**.** Given two integers a and $n > 0$ there exist integers q and r such that $a = qn + r$ and $0 \leq r \leq n - 1$.

This principle is really what we call the long division method of dividing an integer by another. For example dividing 47 by 5 gives us 9 (*quotient*) and *remainder* 2, hence $47 = 9 \times 5 + 2$. This remainder r clearly has to be smaller than the *divisor* n, else the long division process must continue. In particular $r = 0$ if and only if $a = nk$ for some $k \in \mathbb{Z}$, in which case $a \equiv 0 \,(\operatorname{mod} n)$. More generally, following the above theorem, we have $a \equiv r \,(\operatorname{mod} n)$.

Proposition 2.2. For a given $n > 0$, there are exactly n congruence classes of $\mathbb{Z}$ given by $[0]_n, [1]_n, [2]_n, \ldots, [n-1]_n$.

Proof. By the Division Algorithm, each integer a belongs to one of these classes, hence there are at most n of them. To complete the proof we show that these n classes are all distinct. If it were not so then two of them, say $0 \le i < j \le n-1$ satisfy the relation $i \equiv j \pmod{n}$, or $j - i = nk$, which is impossible as $1 \le j - i \le n - 1$. ▽

Definition. The set of *modular integers* $\mathbb{Z}_n$ is the set consisting of the n congruence classes under congruence mod n:

$$\mathbb{Z}_n = \{\, [0]_n, [1]_n, [2]_n, \ldots, [n-1]_n \}$$

And then we define a binary operation $+$ on this set, called *addition mod n*, by letting

$$[a]_n + [b]_n = [a+b]_n$$

We have to show first that this is well-defined, meaning that different choices of a, b for the same classes $[a]_n, [b]_n$ should not yield a different sum. This follows since $[a]_n = [a']_n$ and $[b]_n = [b']_n$ imply $a - a' = nk$ and $b - b' = nh$ hence $(a+b) - (a'+b') = n(k+h)$, thus $a + b \equiv a' + b' \pmod{n}$ and therefore

$$[a']_n + [b']_n = [a' + b']_n = [a+b]_n = [a]_n + [b]_n$$

We are now ready to prove the main result.

Theorem 2.3. The set $\mathbb{Z}_n$ is an abelian group under addition mod n.

Proof. The commutative property is inherited from the ordinary addition used in the definition. Concerning the requirements to be a group, we verify:

1) For every three classes, $[a]_n + ([b]_n + [c]_n) = [a]_n + [b+c]_n = [a + (b+c)]_n = [(a+b)+c]_n = [a+b]_n + [c]_n = ([a]_n + [b]_n) + [c]_n$.

2) The identity element of $\mathbb{Z}_n$ is $[0]_n$ since $[a]_n + [0]_n = [a+0]_n = [a]_n$ for all $[a]_n \in \mathbb{Z}_n$.

3) For each $[a]_n \in \mathbb{Z}_n$, we have $-[a]_n = [-a]_n$ since $[a]_n + [-a]_n = [a-a]_n = [0]_n$. ▽

Remark. From now on, we shall simplify the notations quite drastically. We write $\mathbb{Z}_n = \{0, 1, 2, \ldots n-1\}$ while we really mean that each element is a congruence class mod n—which is an infinite set of integers! From now on let us agree that *the group* $\mathbb{Z}_n$ refers to this group of modular integers under addition mod n.

Example. With $n = 4$ we have $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ where the addition mod 4 produces the following *multiplication table*—just a name, despite the fact that the operation here is addition! To avoid confusion, a multiplication table is better called a *Cayley table.*

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

To avoid ambiguity, instead of writing $2 + 3 = 1$ (which really means $[2]_4 + [3]_4 = [5]_4$) we may sometimes write $2 +_4 3 = 1$, or alternatively $2 + 3 \equiv 1 \pmod{4}$.

Exercise 2. Complete this homework set before we continue to the next section.

1) Draw the Cayley table for the group (a) $\mathbb{Z}_5$ (b) $\mathbb{Z}_2 \times \mathbb{Z}_2$ (c) $\mathbb{Z}_2 \times \mathbb{Z}_3$ (d) $\mathbb{Z}_3 \times \mathbb{Z}_4$.

3 The Group U_n

We continue with the example of $\mathbb{Z}_n$ but this time we introduce a different operation: *multiplication mod n*. For $[a]_n, [b]_n \in \mathbb{Z}_n$ we define $[a]_n[b]_n = [ab]_n$. As before we show first that this is well-defined. Let $[a]_n = [a']_n$ and $[b]_n = [b']_n$. Then $a = a' + nk$ and $b = b' + nh$, hence $ab = a'b' + n(a'h + b'k + nkh)$, that is $ab \equiv a'b' \pmod{n}$. Thus

$$[a']_n[b']_n = [a'b']_n = [ab]_n = [a]_n[b]_n$$

Once again we return to the simplified notation $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$. For example with $n = 4$, we have $2 \times 3 \equiv 2 \pmod{4}$. The complete table of multiplication mod 4 in $\mathbb{Z}_4$ is given below.

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

We can see that in general 1 acts as identity, in which case 0 and 2 have no inverse in $\mathbb{Z}_4$. In fact, $\mathbb{Z}_n$ is not a group under this operation, but we shall proceed to find a subset of $\mathbb{Z}_n$ which does form a group under multiplication mod n.

Definition. Two integers m, n are said to be *relatively prime* when they have no common factors larger than 1. For example 12 and 25 are relatively prime, but 12 and 27 are not since they have a common factor of 3.

Lemma 3.1. The integers m, n are relatively prime if and only if $mx + ny = 1$ for some integers x, y.

Proof. Let d be a common factor of m and n. This means that both m/d and n/d are integers, hence the quantity $mx + ny$ is a multiple of d for any integers x, y. In particular if $mx+ny = 1$ then d divides 1, hence $d = \pm 1$ and m, n are relatively prime.

Conversely, suppose m, n are relatively prime. Let $L = \{mx + ny \mid x, y \in \mathbb{Z}\}$ and let $c = mx_0 + ny_0$ be the least positive element in L. We claim that c divides m. To see why, use the Division Algorithm: $m = qc + r$ with $0 \leq r \leq c - 1$. Then $r = m - qc = m - q(mx_0 + ny_0) = m(1 - qx_0) + n(-qy_0) \in L$. This is impossible as c is supposedly the least, unless $r = 0$. By symmetry, we conclude that c divides n as well. Being a common factor of m and n, then $c = 1$, hence $mx_0 + ny_0 = 1$. ▽

Note that n is relatively prime to m if and only if n is relatively prime to every integer $a \in [m]_n$. This is true since if $a = nk + m$, then $mx + ny = 1$ if and only if $ax + n(y - kx) = 1$.

Corollary 3.2. The integers m, n are relatively prime if and only if there exists an integer b such that $mb \equiv 1 \pmod{n}$, in which case b is also relatively prime to n.

Proof. Note that the equation $mx + ny = 1$ is equivalent to $[m]_n[x]_n = [1]_n$ in $\mathbb{Z}_n$. ▽

Lemma 3.3. Suppose n is relatively prime both to m and to m'. Then n is relatively prime to mm'.

Proof. Let $mx+ny=1$ and $m'x'+ny'=1$ for some integers x, y, x', y'. Multiply these two equations together:

$$mm'(xx') + n(mxy' + m'x'y + nyy') = 1$$

and by the lemma, this means mm' and n are relatively prime. ▽

Definition. Let U_n denote the subset of $\mathbb{Z}_n$ consisting of the classes of m for which m is relatively prime to n.

For example, $U_{10} = \{1, 3, 7, 9\}$. We are now ready to show that this is the subset which forms a group under multiplication mod n.

Theorem 3.4. The set U_n is an abelian group under multiplication mod n.

Proof. The lemma shows that the product of two elements in U_n is again in U_n. Associativity and commutativity follow from those of ordinary multiplication used in the definition. The integer 1 is relatively prime to n and $[1]_n$ is the identity element of U_n. Lastly, the lemma shows that each element of U_n has an inverse element. ▽

Example. The group $U_{10} = \{1, 3, 7, 9\}$ has Cayley table given below.

×	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

Remark. The elements in $\mathbb{Z}_n$ which have a multiplicative inverse, i.e., those that are relatively prime to n, are otherwise called the *units* of $\mathbb{Z}_n$—thus the notation for U_n. Henceforth we simply say *the group* U_n to refer to this group of units in $\mathbb{Z}_n$, where the operation is understood multiplication mod n.

Lemma 3.5 (Euclid's Lemma)**.** If m and n are relatively prime, and $mk \equiv 0 \pmod{n}$ for some integer k, then $k \equiv 0 \pmod{n}$.

Proof. Exercise. ▽

Exercise 3. Complete this homework set before we continue to the next section.

1) Construct the Cayley table for the group (a) U_9 (b) U_{11} (c) $\mathbb{Z}_2 \times U_8$ (d) $U_{12} \times \mathbb{Z}_3$.
2) Find a^{-1} for the group element $a \in G$: (a) $7 \in U_9$ (b) $5 \in U_{11}$ (c) $(1, 3) \in \mathbb{Z}_3 \times U_8$ (d) $(11, 2) \in U_{12} \times \mathbb{Z}_4$.
3) Let $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid a \neq 0\}$. Prove that $\mathbb{Z}_n^*$ is a group under multiplication mod n if and only if n is a prime. (Note: a prime number is an integer larger than 1 that cannot be factored into smaller numbers.)
4) Suppose that m and n are relatively prime. If $k \equiv 0 \pmod{m}$ and $k \equiv 0 \pmod{n}$, prove that $k \equiv 0 \pmod{mn}$.

4 Subgroups

Definition. A subset H of a group G is called a *subgroup* of G if H is itself a group under the same binary operation inherited from G.

Example. We illustrate the idea with several examples.

1) We know that the sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are all groups under addition. In this case $\mathbb{Z}$ is a subgroup of $\mathbb{Q}$, which is a subgroup of $\mathbb{R}$, which is a subgroup of $\mathbb{C}$.

2) The set $\mathbb{Q}^*$ under multiplication is a group and a subgroup of $\mathbb{R}^*$. The subset $\mathbb{Z}^*$ is not a subgroup of $\mathbb{Q}^*$ because it is not a group under multiplication.

3) The set $\mathbb{Q}^+$ of positive rational numbers under multiplication is a subgroup of $\mathbb{Q}^*$. So is $\mathbb{R}^+$, the set of positive real numbers, a subgroup of $\mathbb{R}^*$.

4) The subset $2\mathbb{Z}$ of even numbers is a subgroup of $\mathbb{Z}$ under addition. You can verify that adding two even numbers gives another even number, and that the three group axioms hold in $2\mathbb{Z}$.

5) The set $\{1, -1\}$ forms a group under multiplication, so it is a subgroup of the group $\mathbb{Q}^*$. Although $\{1, -1\}$ is also a subset of $\mathbb{Z}^*$, we cannot say that $\{1, -1\}$ is a subgroup of $\mathbb{Z}^*$ because $\mathbb{Z}^*$ is not a group under multiplication.

6) Every group is a subgroup of itself.

7) Every group has a *trivial subgroup* consisting of only the identity element $\{e\}$.

8) The subset U_n is not a subgroup of $\mathbb{Z}_n$ even though both of them are groups, because they are defined with different binary operations.

9) The set $M(2, \mathbb{Z})$ is a subgroup of $M(2, \mathbb{R})$ under matrix addition.

10) The group $GL(2, \mathbb{R})$ under matrix multiplication has a subgroup given by $SL(2, \mathbb{R})$ consisting of 2×2 matrices with determinant ± 1.

Lemma 4.1. Let H be a subgroup of a group G.

1) The identity element of H is that of G.

2) For each $a \in H$, its inverse in H is the same $a^{-1} \in G$.

Proof. In class. $\triangledown$

Theorem 4.2. A non-empty subset H of a group G is a subgroup if and only if $ab^{-1} \in H$ whenever $a, b \in H$.

Proof. Necessity is clear. Suppose the required condition is satisfied in H. Associativity in H is inherited from G. There is at least one element $a \in H$, hence $aa^{-1} = e \in H$. This is the identity element in H according to the lemma. Also for each $a \in H$ we have $ea^{-1} = a^{-1} \in H$ and this is the inverse of a in H by the lemma. Last but not least, we have to verify that $a, b \in H$ implies $ab \in H$. But since $b \in H$ implies $b^{-1} \in H$ then $a, b \in H$ implies $a(b^{-1})^{-1} = ab \in H$. $\triangledown$

Example. The set $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$, under addition, obeys the condition of Theorem 4.2, since $nk+(-nj) = n(k-j) \in n\mathbb{Z}$. Thus $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$. We call the elements of $n\mathbb{Z}$ *multiples* of n. Note that multiples of n are really members of the congruence class $[0]_n$. In particular, $2\mathbb{Z}$ is the subgroup of even numbers under addition.

Remark. Theorem 4.2 is traditionally called *the One-Step Subgroup Test.* Alternately, one can perform a subgroup test using *the Two-Step Subgroup Test,* as follows.

Theorem 4.3. *A non-empty subset H of a group G is a subgroup if and only if (1) $ab \in H$ for all $a, b \in H$ and (2) $x^{-1} \in H$ for all $x \in H$.*

Proof. In class. ▽

Proposition 4.4. *If H and K are subgroups of G then $H \cap K$ is also a subgroup of G. More generally, the intersection of any collection of subgroups is again a subgroup.*

Proof. Exercise. ▽

Exercise 4. Complete this homework set before we continue to the next section.

1) Prove that H is a subgroup of G for the given $H \subseteq G$: (a) $\{5n \mid n \in \mathbb{Z}\} \subseteq \mathbb{Z}$ (b) $\{\pi^n \mid n \in \mathbb{Z}\} \subseteq \mathbb{R}^*$ (c) $\{A \mid \det A = \pm 1\} \subseteq GL(2, \mathbb{R})$ (d) $\{a+bi \mid a^2+b^2 = 1\} \subseteq \mathbb{C}^*$.
2) Let H be a finite non-empty subset of a group G. Prove that H is a subgroup if and only if $ab \in H$ for all $a, b \in H$.
3) Find a non-trivial example of a group H such that $\mathbb{Z} \subseteq H \subseteq \mathbb{Q}$.
4) For any $a \in G$, the *centralizer* of a in G is defined by $C(a) = \{x \in G \mid ax = xa\}$. Show that $C(a)$ is a subgroup of G, and conclude that the *center* of a group, $Z(G) = \{x \in G \mid ax = xa \text{ for all } a \in G\}$ is also a subgroup of G, upon observing that $Z(G) = \bigcap C(a)$ where the intersection is taken over all the elements $a \in G$.

5 Cyclic Groups

Definition. Let G be a group and $a \in G$. For each integer $n > 0$, we define a^n recursively by $a^1 = a$ and $a^n = a^{n-1}a$. Moreover, let $a^0 = e$ and $a^{-n} = (a^{-1})^n$.

Proposition 5.1. *The following statements hold, for every $m, n \in \mathbb{Z}$.*

1) $a^{-n} = (a^n)^{-1}$

2) $a^m a^n = a^{m+n} = a^n a^m$

3) $(a^m)^n = a^{mn} = (a^n)^m$

Proof. In class. ▽

Definition. Let G be a group and $a \in G$. We define the set $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$ and will prove that this set is a subgroup of G, called the *cyclic subgroup generated by a.*

Theorem 5.2. *For any element $a \in G$, the set $\langle a \rangle$ is an abelian subgroup of G.*

Proof. Elements of $\langle a \rangle$ are of the form a^k for some $k \in \mathbb{Z}$. In particular $a^0 = e \in \langle a \rangle$. If $a^j, a^k \in \langle a \rangle$ then $a^j(a^k)^{-1} = a^j a^{-k} = a^{j-k} \in \langle a \rangle$. Hence $\langle a \rangle$ is a subgroup of G by Theorem 4.2. Commutativity is given by the proposition. (How?) ▽

Remark. When the operation in G is addition, we have $a^k = a + a + \cdots + a$ (with k terms). In that case, we prefer the notation ka to a^k. For example, the subgroup $2\mathbb{Z}$ of $\mathbb{Z}$ under addition is really the cyclic subgroup generated by 2, and in general, $n\mathbb{Z} = \langle n \rangle$.

Definition. Let G be a group. If there exists an element $a \in G$ such that $\langle a \rangle = G$, then we call the group G *cyclic* and call a a *generator* of G.

We have seen that a cyclic group is necessarily abelian but, of course, we do not expect all abelian groups to be cyclic.

Example. The group $\mathbb{Z}$ under addition is a cyclic group generated by 1. Similarly $\mathbb{Z}_n = \langle 1 \rangle$ for all $n > 0$, under addition mod n. Another example is $U_5 = \{1, 2, 3, 4\}$ under multiplication mod 5, where 2 and 3 are both generators.

Theorem 5.3. Any subgroup of a cyclic group is again cyclic.

Proof. Let $G = \langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$ and let H be a subgroup of G. If $H = \{e\}$ then it is cyclic, trivially $H = \langle e \rangle$. Otherwise let n be the least positive integer for which $a^n \in H$. We claim that $H = \langle a^n \rangle$. Well, clearly $\langle a^n \rangle \subseteq H$. Now for each $a^m \in H$ we use the Division Algorithm to write $m = qn + r$ with $0 \leq r \leq n - 1$. Then $a^{qn} = (a^n)^q \in H$ and $a^m(a^{qn})^{-1} = a^{m-qn} = a^r \in H$. But n being the least exponent, this is not possible unless $r = 0$. Hence $a^m = a^{qn} = (a^n)^q \in \langle a^n \rangle$ and it follows that $H = \langle a^n \rangle$. $\bigtriangledown$

Example. Since $\mathbb{Z}$ is cyclic under addition, we conclude that all its subgroups are cyclic, hence of the form $\langle n \rangle = n\mathbb{Z}$. In other words, any subgroup of $\mathbb{Z}$ under addition must be the group of multiples of some integer n. Moreover, as shown in the proof, n is the least positive integer in this subgroup. For example, knowing that the intersection of subgroups is again a subgroup, we have $\langle 4 \rangle \cap \langle 6 \rangle = \langle 12 \rangle$ because 12 is the least positive common multiple of 4 and 6.

Theorem 5.4. As subgroups of $\mathbb{Z}$, if m, n are relatively prime then $\langle m \rangle \cap \langle n \rangle = \langle mn \rangle$.

Proof. Let $\langle c \rangle = \langle m \rangle \cap \langle n \rangle$ where c is the least positive integer in this subgroup. Then by definition $c = mk$ for some integer k, and at the same time also c is a multiple of n. But m, n relatively prime implies, by Euclid's Lemma, that k is multiple of n. Hence c is a multiple of mn. Being the least, $c \leq |mn|$ so $c = |mn|$ and $\langle c \rangle = \langle mn \rangle$. $\bigtriangledown$

Remark. Unlike $\mathbb{Z}_n$, the group U_n is not always cyclic. In number theory, a generator for U_n, if cyclic, goes by the name *primitive root.* It can be shown that primitive roots exist if and only if $n = 2, 4, p^k$, or $2p^k$, where p is any prime number larger than 2 and k is any positive integer. So these are the only values of n for which U_n is a cyclic group. What is a prime number?

Definition. An integer $p > 1$ is *prime* if it is not a multiple of any integer n in the range $1 < n < p$.

The first few prime numbers are 2, 3, 5, 7, 11, 13, . . . Note that a prime p is always relatively prime to all the numbers 1, 2, 3, . . . , $p - 1$, hence $U_p = \{1, 2, 3, \ldots, p - 1\}$.

Exercise 5. Complete this homework set before we continue to the next section.

1) Find all the generators for the cyclic group (a) $\mathbb{Z}_7$ (b) $\mathbb{Z}_8$ (c) U_9 (d) U_{10}.
2) Prove cyclic or not cyclic, for the group (a) U_{15} (b) $\mathbb{Z}_3 \times U_5$ (c) $\mathbb{Z}_2 \times \mathbb{Z}_4$ (d) $U_{10} \times U_6$.
3) Give an example where G and H are both cyclic groups such that $G \times H$ is cyclic, and another example where $G \times H$ is not cyclic.
4) If a group has only 3 elements, prove that it must be cyclic.

6 Cosets

Definition. Let H be a subgroup of a group G. For elements $a, b \in G$, define the relation $a \sim b$ if and only if $ab^{-1} \in H$.

We will show that this $\sim$ defines an equivalence relation on G. For example if $G = \mathbb{Z}$ with addition and $H = \langle n \rangle$, then $a \sim b$ if and only if $a - b \in \langle n \rangle = [0]_n$. But this is the relation $a \equiv b \,(\mathrm{mod}\, n)$ we saw in Section 2.

Proposition 6.1. Let H be a subgroup of a group G, and write $a \sim b$ if and only if $ab^{-1} \in H$. Then the set $R = \{(a, b) \in G \times G \mid a \sim b\}$ is an equivalence relation on G.

Proof. In class. ▽

Definition. We call the equivalence class of $a \in G$ under the relation $\sim$ the *coset* of a in G with respect to the subgroup H, which is given by

$$\begin{aligned} Ha &= \{b \in G \mid b \sim a\} \\ &= \{b \in G \mid ba^{-1} \in H\} \\ &= \{b \in G \mid ba^{-1} = h,\ h \in H\} \\ &= \{b \in G \mid b = ha,\ h \in H\} \\ &= \{ha \mid h \in H\} \end{aligned}$$

Hence, for the relation $a \equiv b \,(\mathrm{mod}\, n)$ on $\mathbb{Z}$, where $H = \langle n \rangle$, the cosets come in the form $\langle n \rangle a = \{h + a \mid h \in \langle n \rangle\} = \{nk + a \mid k \in \mathbb{Z}\} = [a]_n$, i.e., the congruence classes mod n. From the properties of equivalence classes, we conclude that these cosets form a partition for the group G. For one thing this means that every element $a \in G$ belongs to exactly one coset. Other facts are recorded below.

Proposition 6.2. Let H be a subgroup of a group G. Let $a, b \in G$.

1) $a \in Ha$ and, moreover, $b \in Ha$ if and only if $ab^{-1} \in H$.

2) $Ha = Hb$ if and only if $ab^{-1} \in H$. In particular, $Ha = H$ if and only if $a \in H$.

3) $Ha \cap Hb = \phi$ if and only if $ab^{-1} \notin H$.

4) $\bigcup\{Ha \mid a \in G\} = G$.

Definition. How many different cosets are there? Denote this quantity by $[G{:}H]$ and call it the *index* of H in G, if it is finite, otherwise let $[G{:}H] = \infty$. Also denote the number of elements in G by $|G|$ and call this quantity the *order* of G. We say the group G is *finite* or *infinite* depending on $|G|$, and for the latter case we write $|G| = \infty$.

Example. Let $G = \mathbb{Z}_{12}$ and $H = \langle 9 \rangle = \{9, 6, 3, 0\}$. We can check that $[\mathbb{Z}_{12}{:}\langle 9 \rangle] = 3$:

$$\begin{aligned} \langle 9 \rangle + 0 &= \{9, 6, 3, 0\} \\ \langle 9 \rangle + 1 &= \{10, 7, 4, 1\} \\ \langle 9 \rangle + 2 &= \{11, 8, 5, 2\} \end{aligned}$$

and note that any other coset of the form $\langle 9 \rangle + a$ is a duplicate of one of these three, e.g., $\langle 9 \rangle + 5 = \{2, 11, 8, 5\} = \langle 9 \rangle + 2$.

Lemma 6.3. Let G be a group and H a subgroup. For each $a \in G$, we have $|Ha| = |H|$.

Proof. Each element in Ha is of the form ha for some $h \in H$. Moreover $ha = h'a$ implies $h = h'$ by the cancellation law. Hence either both $|Ha|$ and $|H|$ are infinite, or both finite and equal. $\triangledown$

Definition. A nonzero integer n *divides* m if $m = nk$ for some integer k. This is equivalent to having m a multiple of n, i.e., $m \in [0]_n = \langle n \rangle$ when $n > 0$. We also say, in this case, that m is *divisible* by n, or that n is a *divisor* or a *factor* of m.

Theorem 6.4 (Lagrange's Theorem)**.** The order of any subgroup H of a finite group G is a divisor of $|G|$. In particular $|G|/|H| = [G{:}H]$.

Proof. Let G be a finite group and H a subgroup of G. There can be only finitely many cosets in G with respect to H, say $k = [G{:}H]$ of them. By the lemma we have $|H|k = |G|$, hence $|H|$ divides $|G|$. $\triangledown$

Corollary 6.5. A group of prime order is cyclic and, furthermore, any non-identity element is a generator.

Proof. Let G be a group such that $|G| = p$, a prime and let $a \in G$. By Lagrange's Theorem the order of $\langle a \rangle$ divides $|G|$. But $|\langle a \rangle| \neq 1$ unless $a = e$, otherwise $|\langle a \rangle| = p$ and so $\langle a \rangle = G$. $\triangledown$

Definition. Let G be a group and $a \in G$. The *order* of a, denoted by $|a|$, is the least integer $n > 0$ such that $a^n = e$ if such n exists, otherwise let $|a| = \infty$.

Under multiplication mod 5, for instance, we have $2^2 \equiv 4$, $2^3 \equiv 3$, $2^4 \equiv 1$; hence $|2| = 4$ in the group U_5.

Lemma 6.6. Let a be an element of a group G. Then $|a| = |\langle a \rangle|$.

Proof. Assume first $|a| = n$, hence $a^n = e$. Let $H = \{a, a^2, \ldots, a^n\}$ and claim that $\langle a \rangle = H$. It suffices to show that all powers of a belong to H. Given a^m for any integer m, we apply the Division Algorithm to write $m = qn + r$ where $0 \leq r \leq n - 1$. Then $a^m = (a^n)^q a^r = a^r \in H$.

Next we show that the elements $a, a^2, \ldots, a^n$ are all distinct. If ever we had $a^j = a^k$ with $1 \leq j < k \leq n$, then $a^{k-j} = e$, which is impossible as $0 < k - j < n$ while n is supposedly the least number with the property $a^n = e$.

Thus we conclude $|a| = n = |H| = |\langle a \rangle|$. As for the infinite case, note that if $a^j = a^k$ then $a^{j-k} = e$. Thus $|a| = \infty$ implies that the elements $a, a^2, a^3, \ldots$ are all distinct, and so $\langle a \rangle$ will be infinite as well. $\triangledown$

Corollary 6.7. The order of any element in a finite group G is a divisor of $|G|$.

Proof. Let $a \in G$ and $H = \langle a \rangle$ in Lagrange's theorem. Then $|a| = |H|$ divides $|G|$. $\triangledown$

Corollary 6.8. Let G be a finite group and $a \in G$. Then $a^{|G|} = e$.

Proof. Let $|a| = n$, which is finite since G is. We know that $|G| = nk$ for some integer k. Hence $a^{|G|} = (a^n)^k = e^k = e$. $\triangledown$

Definition. For every integer $n > 1$, let $\phi(n)$ denote the number of positive integers up to and relatively prime to n. In other words, $\phi(n) = |U_n|$.

For example $\phi(10) = 4$ since $U_{10} = \{1, 3, 7, 9\}$. Now if we let $G = U_n$ in the last corollary, then we derive the Euler's theorem of number theory. If in addition $n = p$, a prime, then $U_p = \{1, 2, \ldots, p-1\}$ and this is the special case of Fermat's little theorem.

Theorem 6.9 (Euler's Theorem)**.** If a is relatively prime to a positive integer n, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Theorem 6.10 (Fermat's Little Theorem)**.** Let p be a prime and a be any integer which is not a multiple of p. Then $a^{p-1} \equiv 1 \pmod{p}$.

Exercise 6. Complete this homework set before we continue to the next section.

1) Compute $[G{:}H]$ and identify all the cosets with respect to the subgroup $H \subseteq G$: (a) $\langle 9 \rangle \subseteq \mathbb{Z}_{12}$ (b) $\langle 3 \rangle \subseteq U_{13}$ (c) $\langle 5 \rangle \subseteq \mathbb{Z}$ (d) $\langle (4,5) \rangle \subseteq \mathbb{Z}_6 \times U_6$ (e) $\langle (3,3) \rangle \subseteq U_5 \times U_8$.
2) Compute $|a|$ for the group element $a \in G$: (a) $7 \in \mathbb{Z}_{12}$ (b) $5 \in U_{16}$ (c) $(2,2) \in \mathbb{Z}_8 \times \mathbb{Z}_6$ (d) $(2,2) \in \mathbb{Z}_5 \times U_{11}$
3) Prove that the group $U_{17} \times U_{19}$ is not cyclic.
4) Let H and K be two finite subgroups of G. Prove that if $|H|$ and $|K|$ are relatively prime, then $H \cap K = \{e\}$.

7 Finite Cyclic Groups

In this section we seek to identify the order of each element of a given finite cyclic group G. Since every subgroup of G is generated by one element, as G itself is, such knowledge will also lead to the classification of all the subgroups of G.

Lemma 7.1. Let $a \in G$, not assumed cyclic. Then $a^k = e$ if and only if $|a|$ divides k.

Proof. Let $|a| = n$ and write $k = qn + r$ with $0 \le r < n$. We have $a^k = (a^n)^q a^r = a^r$. By the minimality of n, then $a^k = e$ if and only if $r = 0$. ▽

Definition. The *greatest common divisor* of two integers m and n, written $\gcd(m, n)$, is the largest integer which divides both m and n. This quantity always exists (unless $m = n = 0$) and is at least 1. In particular, $\gcd(m, n) = 1$ if and only if m and n are relatively prime.

Theorem 7.2. Suppose $a \in G$, not assumed cyclic, such that $|a| = n$. Then $|a^m| = n/\gcd(m, n)$.

Proof. Let $|a^m| = k$. Since $\langle a^m \rangle$ is a subgroup of $\langle a \rangle$, Lagrange's theorem says that k divides n, so we write $k = n/d$ for some d. This d must be the largest divisor of n such that $(a^m)^{n/d} = e$. Meanwhile, the lemma requires that $|a| = n$ divide $m(n/d) = mk$. As $n = dk$, it follows that d must divide m. Thus d is the largest common divisor of m and n with condition that $a^{mn/d} = e$. This condition actually holds for any divisor of m because $a^{mn/d} = (a^n)^{m/d} = e$; hence choosing $d = \gcd(m, n)$ yields the minimal correct value of k, the order of a^m, i.e., $k = n/\gcd(m, n)$. ▽

Corollary 7.3. Suppose that $G = \langle a \rangle$, of order n. Then $G = \langle a^m \rangle$ if and only if m and n are relatively prime.

Proof. $\langle a^m \rangle = \langle a \rangle$ if and only if $|a^m| = |a| = n$, if and only if $\gcd(m, n) = 1$. ▽

Corollary 7.4. Let m represent an integer as well as an element of $\mathbb{Z}_n$. Then $\mathbb{Z}_n = \langle m \rangle$ if and only if $\gcd(m, n) = 1$, i.e., if and only if $m \in U_n$.

Proof. Simply let $G = \mathbb{Z}_n = \langle 1 \rangle$ in the above corollary. $\triangledown$

Example. Consider $\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. The elements relatively prime to 10 are 1, 3, 7, 9. For each of these, we have

$$\begin{aligned}
\langle 1 \rangle &= \{1, 2, 3, 4, 5, 6, 7, 8, 9, 0\} \\
\langle 3 \rangle &= \{3, 6, 9, 2, 5, 8, 1, 4, 7, 0\} \\
\langle 7 \rangle &= \{7, 4, 1, 8, 5, 2, 9, 6, 3, 0\} \\
\langle 9 \rangle &= \{9, 8, 7, 6, 5, 4, 3, 2, 1, 0\}
\end{aligned}$$

Note that other elements will not generate the group, e.g., $\langle 4 \rangle = \{4, 8, 2, 6, 0\}$.

Theorem 7.5. Let G be a cyclic group of order n, and let d be any positive divisor of n. Then G has a unique subgroup of order d.

Proof. Let $a \in G$ such that $G = \langle a \rangle$. By Lagrange's theorem, we may let $dk = n$ for some integer k. Hence, by Theorem 7.2 we have $|a^k| = n/k = d$, thus the subgroup $H = \langle a^k \rangle$ of order d. If there were another (cyclic) subgroup $\langle a^m \rangle$ of order d, then Theorem 7.2 again gives $\gcd(m, n) = k$ so k divides m, implying that $a^m \in \langle a^k \rangle$ and $\langle a^m \rangle \subseteq H$. Therefore, $\langle a^m \rangle = H$ as both have equal finite order. $\triangledown$

Theorem 7.6. Let $G = \langle a \rangle$, of order n. Including a, there are exactly $\phi(n)$ generating elements of G. Moreover, for every positive divisor d of n, there exist exactly $\phi(d)$ elements in G of order d.

Proof. Write $G = \{a, a^2, \ldots, a^n = e\}$. By Corollary 7.3, a^m generates G if and only if $m \in U_n$. Their number is given by $|U_n| = \phi(n)$. Now if d divides n, say $dk = n$, then $|a^k| = n/k = d$. By the preceding lemma, every element of order d is a generator of this subgroup $\langle a^k \rangle$ of order d. By the same reasoning, there are $\phi(d)$ such elements. $\triangledown$

Remark. By Corollary 6.7, every element in such a group has order a divisor of n. The above theorem then yields a known identity of number theory involving the phi-function: $\sum \phi(d) = n$, where the sum is over all positive integers d that divide n.

Example. Since every subgroup of a cyclic group is again cyclic, all these results apply to any finite cyclic group G as well as all its subgroups and its sub-subgroups. The *subgroup lattice* is a way we can diagram these subgroup relations. The following is the subgroup lattice for the group $\mathbb{Z}_{12}$. Note that $\langle 1 \rangle = \mathbb{Z}_{12}$ and that $\langle 12 \rangle = \langle 0 \rangle = \{0\}$.

$$\begin{tikzcd}
& & \langle 1 \rangle \arrow[dl, dash] \arrow[dr, dash] & \\
& \langle 2 \rangle \arrow[dl, dash] \arrow[dr, dash] & & \langle 3 \rangle \arrow[dl, dash] \\
\langle 4 \rangle \arrow[dr, dash] & & \langle 6 \rangle \arrow[dl, dash] & \\
& \langle 12 \rangle & &
\end{tikzcd}$$

Exercise 7. Complete this homework set before we continue to the next section.

1) Let G and H be two finite cyclic groups.

   a) Prove that if $\gcd(|G|, |H|) = 1$, then $G \times H$ is cyclic.
   b) Prove that if $\gcd(|G|, |H|) > 1$, then $G \times H$ is not cyclic.
   c) If cyclic, prove that $G \times H = \langle(a, b)\rangle$ if and only if $G = \langle a\rangle$ and $H = \langle b\rangle$.
   d) If $\gcd(m, n) = 1$, prove that $\phi(mn) = \phi(m)\phi(n)$ by letting $G = \mathbb{Z}_m$ and $H = \mathbb{Z}_n$.

2) Count how many generators for the cyclic group (a) $\mathbb{Z}_{36}$ (b) U_{17} (c) U_{27} (d) $\mathbb{Z}_5 \times U_{10}$.
3) Draw the subgroup lattice for the cyclic group (a) $\mathbb{Z}_{24}$ (b) $\mathbb{Z}_4 \times \mathbb{Z}_5$ (c) U_{17} (d) U_{18}.
4) Find all the elements $a \in \mathbb{Z}_{224}$ of order (a) 8 (b) 12 (c) 14 (d) 16.

8 Normal Subgroups

Had we defined the equivalence relation $a \sim b$ to be $b^{-1}a \in H$ then the coset of a would have looked different, i.e., $aH = \{ah \mid h \in H\}$. We call such the *left coset* of a in G with respect to the subgroup H, to be distinguished from the *right coset* Ha of the previous section. This differentiation would not be necessary if G is abelian, in which case $aH = Ha$ for all $a \in G$, or if H is a normal subgroup, below.

Definition. Let G be a group. A subgroup N of G is called *normal* if $aN = Na$ for every $a \in G$.

For abelian groups, all subgroups are trivially normal. (Hence, normal subgroups are special only in the non-abelian case.) The converse, however, is false: see Exercise 13.1 for an example of a non-abelian group whose subgroups are all normal.

Proposition 8.1. A subgroup N of G is normal if and only if $ana^{-1} \in N$ for every $a \in G$ and $n \in N$.

Proof. Suppose N is normal. Then $an \in aN = Na$, hence $an = n'a$ for some $n' \in N$. It follows that $ana^{-1} = n'aa^{-1} = n' \in N$. Conversely, suppose that $ana^{-1} \in N$ for every $a \in G$ and $n \in N$. Then

$$\begin{aligned} b \in Na &\leftrightarrow ab^{-1} \in N \\ &\leftrightarrow b^{-1}(ab^{-1})b \in N \\ &\leftrightarrow b^{-1}a \in N \\ &\leftrightarrow b \in aN \end{aligned}$$

which shows that $Na = aN$. ▽

Definition. For any subsets A and B of a group G, we define the product $AB = \{ab \mid a \in A, b \in B\}$. In particular when $B = \{b\}$ we write $AB = Ab$, which coincides with the notion of a (right) coset when A is a subgroup. Note that associativity in G implies that $A(BC) = (AB)C$ for any three subsets A, B, C.

Lemma 8.2. Let N be a normal subgroup of G. Then for every $a, b \in G$,

1) $NN = N$

2) $N(Na) = (Na)N = Na$

3) $(Na)(Nb) = N(ab)$

Proof. We have $NN = \bigcup\{Nn \mid n \in N\} = N$, since for any subgroup (not necessarily normal) $Ha = H$ if and only if $a \in H$. Then

$$(Na)(Nb) = N(aN)b = N(Na)b = (NN)(ab) = N(ab)$$

In particular with $b = e$, $(Na)N = Na$ and $N(Na) = Na$. $\bigtriangledown$

Definition. With N a normal subgroup of G, let G *mod* N be the set of all cosets in G with respect to N, which is written $G/N = \{Na \mid a \in G\}$. We also introduce the operation $(Na)(Nb) = N(ab)$ in this set G/N, which will then become a group of order $[G{:}N]$. The group G/N is called the *quotient group* or *factor group* of G mod N.

Theorem 8.3. For any normal subgroup N of a group G, the set G/N forms a group under the operation $(Na)(Nb) = N(ab)$ for every $a, b \in G$.

Proof. We show first that this operation is well-defined. Suppose that $Na = Na_2$ and $Nb = Nb_2$. These are equivalent to having $aa_2^{-1}, bb_2^{-1} \in N$. Since N is normal, then $c = a_2(bb_2^{-1})a_2^{-1} \in N$. Hence $aa_2^{-1}c = ab(a_2b_2)^{-1} \in N$, meaning that $(ab) \sim a_2b_2$ and so $N(a)N(b) = N(ab) = N(a_2b_2) = N(a_2)N(b_2)$. Now for the group axioms:

1) Associative: $Na((Nb)(Nc)) = (Na)N(bc) = N(a(bc)) = N((ab)c) = N(ab)N(c) = (N(a)N(b))N(c)$.

2) Identity: The identity element in G/N is $N = Ne$.

3) Inverse: For each element $Na \in G/N$ its inverse is given by $N(a^{-1})$. $\bigtriangledown$

Example. The group $\mathbb{Z}$ under addition is abelian, hence all its subgroups are normal. Let $N = \langle 2\rangle$, the subgroup of all even numbers. Then $N + a = N$ if a is even. If a and b are both odd then $a - b$ is even and belongs to N, hence $N + a = N + b$. Thus the quotient group $Z/\langle 2\rangle = \{\langle 2\rangle, \langle 2\rangle + 1\} = \{e, o\}$, where e represents the coset of even numbers $[0]_2$ and o the coset of odd numbers $[1]_2$. The Cayley table is,

$+$	e	o
e	e	o
o	o	e

In the next section, we will see that this group is essentially $\mathbb{Z}_2$ in the sense of isomorphism. Also in general we will show that $\mathbb{Z}/\langle n\rangle \approx \mathbb{Z}_n$.

Example. We look at the group U_7 and one of its subgroups, $\langle 6\rangle = \{1, 6\}$. There are three cosets given by $\langle 6\rangle 1 = \langle 6\rangle$, $\langle 6\rangle 2 = \{2, 5\}$, and $\langle 6\rangle 3 = \{3, 4\}$. These three form the factor group $U_7/\langle 6\rangle$ whose Cayley table, represented by 1, 2, 3, respectively, is provided below. Can you identify this group with another familiar group?

$\times$	1	2	3
1	1	2	3
2	2	3	1
3	3	1	2

Exercise 8. Complete this homework set before we continue to the next section.

1) Construct the Cayley table for the factor group G/H for each problem given in Exercise 6.1. (Note that all those groups are abelian, hence normal subgroups.)
2) Prove that the subgroup $SL(2, \mathbb{R})$ is normal in $GL(2, \mathbb{R})$.
3) Let H be a subgroup of G. Prove that if $[G{:}H] = 2$, then H is normal.
4) Let G be a group. Prove that the center subgroup $Z(G)$ is normal and that the factor group $G/Z(G)$ is either trivial or not cyclic.

9 Group Isomorphisms

Definition. A function $\theta : G \to G'$ between two groups is called a *homomorphism* if it satisfies $\theta(ab) = \theta(a)\theta(b)$ for every $a, b \in G$. In such a case, we define the *range* $\theta(G) = \{\theta(a) \mid a \in G\}$ and the *kernel* $\ker(\theta) = \{a \in G \mid \theta(a) = e'\}$, where e' denotes the identity in G'.

We say that a homomorphism preserves the binary operation going from G into G'. Note that the operation $\theta(a)\theta(b)$ is that of G', which is not distinguishable from that of G in the notation but is not assumed the same.

Example. Let us illustrate this idea with a few examples.

1) Let $\theta : \mathbb{Z} \to \mathbb{Z}_n$ be given by $\theta(a) = [a]_n$. This is a homomorphism as $[a+b]_n = [a]_n + [b]_n$. We have $\ker(\theta) = n\mathbb{Z}$ and $\theta(\mathbb{Z}) = \mathbb{Z}_n$.

2) Let $\theta : \mathbb{Z} \to \{\pm 1\}$ such that $\theta(n) = (-1)^n$. Then $\theta(a+b) = (-1)^{a+b} = (-1)^a(-1)^b = \theta(a)\theta(b)$, showing that θ is a homomorphism. Here, $\theta(\mathbb{Z}) = \{\pm 1\}$ and $\ker(\theta) = \langle 2 \rangle$.

3) Let $\theta : \mathbb{R} \to \mathbb{R}^*$ where $\theta(x) = e^x$. We have $e^{x+y} = e^x e^y$ hence θ is a homomorphism, with $\theta(\mathbb{R}) = (0, \infty)$ and $\ker(\theta) = \{0\}$.

Proposition 9.1. Let $\theta : G \to G'$ be a homomorphism from a group G with identity e to another group G' with identity e'.

1) $\theta(e) = e'$ and $\theta(a^{-1}) = \theta(a)^{-1}$ for every $a \in G$.

2) θ is one-to-one if and only if $\ker(\theta) = \{e\}$.

3) $\theta(G)$ is a subgroup of G'.

4) $\ker(\theta)$ is a normal subgroup of G.

Proof. In class. ▽

Definition. A homomorphism $\theta : G \to G'$ is called an *isomorphism* when θ is one-to-one and onto, in which case we say that G and G' are *isomorphic*, written $G \approx G'$. The meaning of onto is, of course, that $\theta(G) = G'$.

Isomorphism really means that the two groups are essentially identical, except for the different labeling of the elements. For example, consider the group with 2 elements, i.e., $G = \{e, a\}$ in which $a^2 = e$. We can see that $G \approx \mathbb{Z}_2$ by identifying $\theta(e) = 0$ and $\theta(a) = 1$. Another illustration, from Example (3) above, the group $\mathbb{R}$ under addition is isomorphic to the sub-interval $(0, \infty)$ under multiplication, by way of the homomorphism function $\theta(x) = e^x$, or the inverse $\theta^{-1}(y) = \ln y$. Thus $\mathbb{R} \approx \mathbb{R}^+$.

Theorem 9.2. Any finite cyclic group of order n is isomorphic to $\mathbb{Z}_n$. Any infinite cyclic group is isomorphic to $\mathbb{Z}$.

Proof. Let $G = \langle a \rangle = \{a^0, a^1, a^2, \ldots, a^{n-1}\}$ where $a \in G$ is of order n. Let $\theta : G \to \mathbb{Z}_n$ be given by $\theta(a^k) = k = [k]_n$. This is a homomorphism since

$$\theta(a^k a^l) = \theta(a^{k+l}) = [k+l]_n = [k]_n + [l]_n = \theta(a^k) + \theta(a^l)$$

Moreover, θ is one-to-one as $\theta(a^k) = [0]_n$ if and only if $k = 0$ and $a^k = e$. Lastly, θ is clearly onto, establishing the isomorphism $G \approx \mathbb{Z}_n$.

If on the other hand $|a| = \infty$, then simply define $\theta(a^k) = k \in \mathbb{Z}$. By a very similar argument, we can show that θ is an isomorphism and $G \approx Z$. ▽

Theorem 9.3 (The Fundamental Homomorphism Theorem)**.** Let $\theta : G \to G'$ be a homomorphism of groups. Then $G/\ker(\theta) \approx \theta(G)$.

Proof. We let $H = \ker(\theta)$ and define the map $\Theta : G/H \to \theta(G)$ according to the rule $\Theta(Ha) = \theta(a)$. This map is well-defined, for if $Ha = Hb$ then $ab^{-1} \in H$, leading to $e' = \theta(ab^{-1}) = \theta(a)\theta(b)^{-1}$ and thus $\theta(a) = \theta(b)$. It is also a homomorphism because

$$\Theta((Ha)(Hb)) = \Theta(H(ab)) = \theta(ab) = \theta(a)\theta(b) = \Theta(Ha)\Theta(Hb)$$

as θ is. It is clear that Θ is onto and furthermore, the fact that $\theta(a) = \theta(b)$ implies $Ha = Hb$ (How?) shows that Θ is one-to-one, hence an isomorphism. $\triangledown$

Example. The following are some examples of isomorphism between groups.

1) From Example (1) previously, $\mathbb{Z}/n\mathbb{Z} \approx \mathbb{Z}_n$.

2) In particular from Example (2), $\mathbb{Z}/2\mathbb{Z} \approx \{\pm 1\} \approx \mathbb{Z}_2$.

3) As a counter-example, we shall demonstrate why $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not isomorphic to $\mathbb{Z}_4$. Note that every element $\alpha \in \mathbb{Z}_2 \times \mathbb{Z}_2$ meets the condition $\alpha^2 = (0, 0)$, the identity of this group. Therefore $\theta(\alpha)^2 = 0 \in \mathbb{Z}_4$—if θ is a homomorphism. But then this θ cannot be onto since $\mathbb{Z}_4$, being cyclic, contains an element of order 4.

Remark. Generally speaking, an isomorphism preserves algebraic structures of the one group onto the other. Properties such as group order, being abelian or cyclic, existence of a particular subgroup, etc., must agree between the two isomorphic groups. In the example of $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_4$, the fact that one is cyclic and the other not is sufficient evidence that no isomorphism can exist between the two groups.

Theorem 9.4 (Chinese Remainder Theorem)**.** Suppose that m and n are relatively prime positive integers. Then $\mathbb{Z}_m \times \mathbb{Z}_n \approx \mathbb{Z}_{mn}$.

Proof. Let $\theta : \mathbb{Z} \to \mathbb{Z}_m \times \mathbb{Z}_n$ be defined by $\theta(a) = (a, a) = ([a]_m, [a]_n)$. The fact that $[a + b] = [a] + [b]$ in each $\mathbb{Z}_m$ and $\mathbb{Z}_n$ makes this function an onto homomorphism. We have $\ker(\theta) = \{a \in \mathbb{Z} \mid a \in [0]_m \cap [0]_n\} = \langle mn \rangle$ by Theorem 5.4. Hence $\mathbb{Z}_m \times \mathbb{Z}_n \approx \theta(\mathbb{Z}) \approx \mathbb{Z}/\langle mn \rangle \approx \mathbb{Z}_{mn}$ by the fundamental homomorphism theorem. $\triangledown$

Remark. The Chinese remainder theorem belongs to number theory. For an illustration, this theorem implies that the congruence $a \equiv b \pmod{12}$ is equivalent to the the simultaneous pair $a \equiv b \pmod 3$ and $a \equiv b \pmod 4$. It also means that the congruences $x \equiv 5 \pmod 7$ and $x \equiv 8 \pmod{11}$ have a unique common solution in $\mathbb{Z}_{77}$.

Corollary 9.5. If m and n are relatively prime, then $\phi(mn) = \phi(m)\phi(n)$.

Proof. Note that $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$ is a unit element (i.e., invertible under multiplication) if and only if $a \in U_m$ and $b \in U_n$. This says that we have $\phi(m)\phi(n)$ such units. Looking at $\mathbb{Z}_{mn}$ on the other hand, we know this number is equal to $|U_{mn}| = \phi(mn)$. $\triangledown$

Exercise 9. Complete this homework set before we continue to the next section.

1) Let G be a group and let $\theta(a) = a^{-1}$ for all $a \in G$. Prove that θ is an isomorphism on G if and only if G is abelian.
2) Let $a \in G$ and $\theta : G \to G$ be given by $\theta(x) = axa^{-1}$ for every $x \in G$. Prove that θ is an isomorphism—this is called the *inner automorphism* of G induced by a.
3) Prove (a) $U_7 \approx U_9 \approx U_{14}$ (b) $\mathbb{R} \approx \mathbb{R}^+$ (c) $U_{15} \not\approx U_{24}$ (d) $\mathbb{Z}_4 \times \mathbb{Z}_4 \not\approx \mathbb{Z}_2 \times \mathbb{Z}_8$.
4) Prove the converse of the Chinese remainder theorem: if m and n are not relatively prime, then $\mathbb{Z}_m \times \mathbb{Z}_n \not\approx \mathbb{Z}_{mn}$.

10 Finite Abelian Groups

The main thing in this section is the classification of all abelian groups of a given order. Such a task shall be carried out effectively by the fundamental theorem of finite abelian groups, whose proof will be provided in a separate handout as a reading assignment.

Theorem 10.1 (The Fundamental Theorem of Finite Abelian Groups)**.** Every finite abelian group is isomorphic to the direct product of cyclic groups.

Before putting this theorem into action, we need to borrow from number theory the fundamental theorem of arithmetic, which states that every positive integer n is a unique product of powers of distinct primes, $n = \prod p_i^{k_i}$. Note that powers of primes in such an expression are pairwise relatively prime:

Definition. The integers $n_1, n_2, \ldots, n_k$ are said to be *pairwise relatively prime* when they are relatively prime in pairs, that is, $\gcd(n_i, n_j) = 1$ whenever $i \neq j$.

The Chinese remainder theorem can now be generalized in a natural way involving three or more copies of finite cyclic groups.

Theorem 10.2 (Chinese Remainder Theorem)**.** If the integers $n_1, n_2, \ldots, n_k$ are pairwise relatively prime then $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k} \approx \mathbb{Z}_{n_1 n_2 \cdots n_k}$.

Hence, by the fundamental theorem, every finite abelian group is isomorphic to the direct product of cyclic groups of a prime power order. This knowledge enables us to classify with ease all abelian groups of a fixed order.

Example. Consider an abelian group of order $400 = 2^4 \times 5^2$. There are only 10 ways in which we can possibly have distinct prime powers whose product is 400, where each choice corresponds to a direct product in the following list.

$$\begin{array}{rr}
\mathbb{Z}_{2^4} \times \mathbb{Z}_{5^2} & \qquad \mathbb{Z}_{2^4} \times \mathbb{Z}_5 \times \mathbb{Z}_5 \\
\mathbb{Z}_{2^3} \times \mathbb{Z}_2 \times \mathbb{Z}_{5^2} & \qquad \mathbb{Z}_{2^3} \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \\
\mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_{5^2} & \qquad \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_5 \times \mathbb{Z}_5 \\
\mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{5^2} & \qquad \mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \\
\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{5^2} & \qquad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5
\end{array}$$

It is not hard to verify that no two of these 10 groups are isomorphic to each other.

Remark. Thus the number of distinct abelian groups of a prime order p^k is given by the $p(k)$, i.e., the number of distinct partitions of the positive integer k. For example, $p(4) = 5$ since there are 5 ways we can partition the number 4, namely (a) $4 = 4$; (b) $4 = 3 + 1$; (c) $4 = 2 + 2$; (d) $4 = 2 + 1 + 1$; and (e) $4 = 1 + 1 + 1 + 1$.

Two immediate consequences of the fundamental theorem are worth mentioning, one of which is an independent theorem due to Cauchy. Be aware, however, that the genuine Cauchy's theorem applies to finite groups in general, not just abelian groups. (See Corollary 13.2.)

Corollary 10.3 (Cauchy's Theorem)**.** Let G be a finite abelian group of order divisible by p, a prime number. Then there exists an element of order p in G.

Proof. The prime p appears in the factorization of $n = |G|$, hence one of the cyclic groups in the product, say the first, is $\mathbb{Z}_{p^k}$ with $k \geq 1$. Since p divides p^k, we have an element of order p in $\mathbb{Z}_{p^k}$, call it a. This gives us an element of order p in G, corresponding to the element $(a, 0, \ldots, 0)$ in the direct product. $\triangledown$

Corollary 10.4. Suppose that G is an abelian group of order n, and that n has no repeated prime factors. Then $G \approx \mathbb{Z}_n$ and hence G is cyclic.

Proof. Then $G \approx \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_k}$ and since all these primes are pairwise relatively prime, the result follows by the Chinese remainder theorem. $\triangledown$

Exercise 10. Complete this homework set before we continue to the next section.

1) List all the abelian groups of order (a) 25 (b) 42 (c) 100 (d) 1200.
2) Count how many abelian groups can have order (a) 5400 (b) 5184 (c) 2310 (d) 1024.
3) Prove (a) $U_8 \approx U_{12}$ (b) $U_{71} \approx \mathbb{Z}_{70}$ (c) $U_{15} \approx U_{16} \approx U_{20}$ (d) $U_{24} \approx \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.
4) Let G be a finite abelian group of order a multiple of d. Prove that G has a subgroup of order d.

11 Permutation Groups

Definition. A *permutation* on a set A means a function $f : A \to A$ which is one-to-one and onto. If the set is given by $A = \{1, 2, 3, \ldots, n\}$ then let S_n denote the set of all permutations on A. It is not hard to see that $|S_n| = n!$ and that S_n forms a group under function composition.[2] We call S_n the *symmetric group* of degree n and call any subgroup of S_n a *permutation group.*

Theorem 11.1 (Cayley's Theorem)**.** Every group is isomorphic to a permutation group.

Sketch of proof. For each $a \in G$ we associate to it $f_a : G \to G$ given by $f_a(x) = ax$ for all $x \in G$. This function f_a is a permutation on G. The set $G' = \{f_a \mid a \in G\}$ is then a group under composition. That $G \approx G'$ can be established by showing that $a \to f_a$ is indeed an isomorphism. $\triangledown$

Remark. If G is a finite group, according to Cayley's theorem, G is isomorphic to a subgroup of S_n, where $n = |G|$. In particular, there can be only finitely many groups, up to isomorphism, of a given finite order.

Example. Consider S_6, the group of $6! = 720$ permutations on $\{1, 2, 3, 4, 5, 6\}$. An element $f \in S_6$ may be expressed in *cyclic notation*, e.g., $f = (1, 2, 5)(3, 6)$, which determines the behaviour of the function f given by

$$\begin{array}{lll} f(1) = 2 & f(2) = 5 & f(3) = 6 \\ f(4) = 4 & f(5) = 1 & f(6) = 3 \end{array}$$

[2] Recall from calculus concerning the composition of two functions f and g which is normally written $g \circ f(x) = g(f(x))$.

Note that 4 is missing in the notation; this is understood as $f(4) = 4$. In general, elements left unchanged by the permutation need not be included in the cyclic notation, except when writing the identity permutation: $e = (1)$. Following convention, composition is read from right to left, and it is generally non-commutative, e.g.,

$$(1,2,5)(3,6) \circ (1,4,6,2) = (1,4,3,6,5)$$
$$(1,4,6,2) \circ (1,2,5)(3,6) = (2,5,4,6,3)$$

Definition. The term *cycle* refers to each bracketed part in a cyclic notation. It is intuitively clear that every permutation can be represented by *disjoint* cycles, that is, where no two cycles have a common element. If a cycle has d elements in it, we call it a *d-cycle*.

For example, the permutation $(1,2,5)(3,6)$ is written in two disjoint cycles: the 3-cycle $(1,2,5)$ and the 2-cycle $(3,6)$. Note that it is not ambiguous to write $(1,2,5)(3,6)$ in place of the composition $(1,2,5) \circ (3,6)$. Moreover,

Proposition 11.2. If f and g are two disjoint cycles then $g \circ f = f \circ g$.

Proposition 11.3. Every permutation is a product of 2-cycles. There is more than one way to express this product, but the parity of the number of 2-cycles that are used is unique, i.e., always even or always odd.

Proof. Note that, for example, $(1,2,3,4,5,6) = (1,2,3,4,5) \circ (5,6)$ and then use induction. To show that parity is unique, first prove that the identity e cannot be written as a product of odd 2-cycles (again by induction). Next observe that $f^{-1} = f$ if f is a 2-cycle. Hence with 2-cycles, if $f_1 f_2 \cdots f_s = g_1 g_2 \cdots g_t$ then $g_t \cdots g_2 g_1 \circ f_1 f_2 \cdots f_s = e$, and so $s + t$ must be even, i.e., s and t are either both odd or both even. $\bigtriangledown$

Definition. A permutation is called *even* or *odd* as it is the product of an even or odd number of 2-cycles. In particular, the even permutations form a subgroup of S_n, called the *alternating group* of degree n and denoted by A_n.

Theorem 11.4. A_n is a subgroup of S_n of order $n!/2$.

Proof. Working with 2-cycles, it is clear that the composition of two even permutations is again even. Furthermore since every 2-cycle is self-inverse, the inverse of a permutation retains its parity. (Why?) Theorem 4.2 then implies that A_n is a subgroup.

Now, what are the cosets induced by A_n? One of them is $eA_n = A_n$. Then consider the coset $(1,2)A_n$. (Despite its appearance, this is a right coset since composition reads right to left. Also, the theorem must assume $n \geq 2$, else $A_1 = S_1 = \{e\}$.) Every odd permutation f belongs to $(1,2)A_n$ because $f^{-1} \circ (1,2)$ is even. These two cosets then make up all of S_n, hence A_n accounts for exactly half of the elements in S_n. $\bigtriangledown$

Exercise 11. Complete this homework set before we continue to the next section.

1) Use the cyclic notation to write all the elements in S_4, separating between the even and the odd permutations.
2) Find all the cosets with respect to the given subgroup $H \subseteq G$: (a) $\langle(1,3,2)\rangle \subseteq A_4$ (b) $\langle(1,4)(2,3)\rangle \subseteq A_4$ (c) $A_3 \subseteq S_3$ (d) $\langle(1,4,2,3)\rangle \subseteq S_4$.
3) Prove that (a) the group S_n is non-abelian for $n \geq 3$ and (b) the subgroup A_n is non-abelian for $n \geq 4$.
4) Prove that the alternating subgroup A_n is normal in S_n, and then draw the Cayley table for the factor group S_n/A_n.

12 The Dihedral Groups

We consider a permutation group which arises in geometry, i.e., the group of symmetries on a regular polygon. Let us label the vertices of a regular n-gon by $1, 2, \ldots, n$. There are n symmetries by rotation of $d^o, 2d^o, 3d^o, \ldots, 360^o$ angles, where $d = 360/n$. Looking at the n vertices, these rotations are respectively given by the permutations $R, R^2, R^3, \ldots, R^n$, where $R = (1, 2, 3, \ldots, n)$ and $R^n = e$. Then there are also reflections along the n axes of symmetry, making a total of $2n$ permutations which form a subgroup D_n of S_n.

Example. We illustrate with $n = 4$, a square. The four reflections are $F_1 = (1, 4)(2, 3)$, $F_2 = (2, 4)$, $F_3 = (1, 2)(3, 4)$, and $F_4 = (1, 3)$; while the four rotations are given by $R = (1, 2, 3, 4)$, $R^2 = (1, 3)(2, 4)$, $R^3 = (1, 4, 3, 2)$, and $R^4 = e$.

The Cayley table for D_4 given below shows how the compositions work. Do not forget that they read right to left, so in our version we have row $\circ$ column, e.g., $R^3 \circ F_1 = (1, 4, 3, 2) \circ (1, 4)(2, 3) = (1, 3) = F_4$—you see this result in the R^3 row (row 3) and F_1 column (column 5).

$\circ$	R	R^2	R^3	R^4	F_1	F_2	F_3	F_4
R	R^2	R^3	R^4	R	F_2	F_3	F_4	F_1
R^2	R^3	R^4	R	R^2	F_3	F_4	F_1	F_2
R^3	R^4	R	R^2	R^3	F_4	F_1	F_2	F_3
R^4	R	R^2	R^3	R^4	F_1	F_2	F_3	F_4
F_1	F_4	F_3	F_2	F_1	R^4	R^3	R^2	R
F_2	F_1	F_4	F_3	F_2	R	R^4	R^3	R^2
F_3	F_2	F_1	F_4	F_3	R^2	R	R^4	R^3
F_4	F_3	F_2	F_1	F_4	R^3	R^2	R	R^4

Theorem 12.1. D_n is a group under composition of functions.

Proof. As a finite subset of S_n, it suffices to show that D_n is closed under composition, meaning that $g \circ f \in D_n$ for all $f, g \in D_n$. This is clear if both f and g are rotations for the rotations form the cyclic subgroup $\langle R \rangle$ of S_n. The Cayley table above suggests that in general $g \circ f$ is a rotation when f and g are both reflections, and that $g \circ f$ is a reflection when f and g are of opposite kind. Although these results may be geometrically intuitive, we leave the proof as an exercise. $\bigtriangledown$

Definition. We fix the notation $D_n = \{R, R^2, \ldots, R^n, F_1, F_2, \ldots, F_n\}$, refering to the R's as rotations and the F's reflections. In particular, we let $R = (1, 2, 3, \ldots, n)$, hence $|R| = n$. This permutation group D_n is called the *dihedral group* of degree n.

Note that since $|D_n| = 2n$, in particular we have $D_3 = S_3$. But in general D_n is a proper subgroup of S_n and is non-abelian as S_n is.

Theorem 12.2. Let p denote a prime number larger than 2. Every group of order $2p$ is isomorphic to either Z_{2p} (if abelian) or to D_p (if non-abelian).

Proof. The abelian case is given by Corollary 10.4. Assume G is a non-abelian group of order $2p$. A non-identity element in G must have order 2 or p (not $2p$ or else G would be cyclic, hence abelian). Not all elements can have order 2, lest G would be abelian (Exercise 1.4) so let $a \in G$ be chosen with $|a| = p$.

Thus G is partitioned into two cosets, $\langle a\rangle$ and $\langle a\rangle b$ for any element $b \notin \langle a\rangle$. Moreover $|b| = 2$ for the following reason. If not then $|b| = p$ and $\langle a\rangle \cap \langle b\rangle = \{e\}$ since a non-trivial common element will generate both. But $\langle a\rangle$ is normal in G (of index 2!) so $\langle a\rangle b^2$ is identity in $G/\langle a\rangle$, that is, $b^2 \in \langle a\rangle$—a contradiction.

We have shown that any non-abelian group of order $2p$ is necessarily of the form $G = \{a, a^2, \ldots, a^p = e, ab, a^2b, \ldots, a^pb = b\}$. To complete the proof, we next show that the binary operation on G is uniquely determined so that up to isomorphism there can be only one such group. Simply note that $|ab| = 2$ since $ab \notin \langle a\rangle$, thus $ab = (ab)^{-1} = b^{-1}a^{-1} = ba^{-1}$. This determines all products in G for they are of the form either $a^i(a^jb^k) = a^{i+j}b^k$ or $(a^ib)(a^jb^k) = a^i(ba^j)b^k = a^i(a^{-j}b)b^k = a^{i-j}b^{k+1}$, where $k = 0$ or 1. $\triangledown$

In the above proof we are shown two more facts about D_n which we shall state and prove again anyhow as follows.

Proposition 12.3. In any dihedral group, the composition of a rotation with a reflection, in either order, is a reflection.

Proof. The cyclic subgroup $\langle R\rangle$ of D_n contains all the n rotations, and it generates two cosets—the other one being the set of all n reflections represented by $F\langle R\rangle$, or $\langle R\rangle F$, for any reflection $F \in D_n$. $\triangledown$

Proposition 12.4. If $F \in D_n$ is a reflection then $F \circ R = R^{n-1} \circ F$.

Proof. Being a reflection, $F \circ R$ is self-inverse, hence $F \circ R = (F \circ R)^{-1} = R^{-1} \circ F$. $\triangledown$

Exercise 12. Complete this homework set before we continue to the next section.

1) Use the cyclic notation to write all the elements of D_n, distinguishing between the rotations and the reflections in each one, for $n =$ (a) 3 (b) 4 (c) 5 (d) 6.
2) Find all the cosets with respect to the given subgroup $H \subseteq G$: (a) $\langle(1,2,3,4)\rangle \subseteq D_4$ (b) $\langle(2,5)(3,4)\rangle \subseteq D_5$ (c) $\langle(1,3,5)(2,4,6)\rangle \subseteq D_6$ (d) $D_4 \subseteq S_4$.
3) Prove that (a) D_n is non-abelian for all $n \geq 3$ and (b) $D_n \subseteq A_n$ if and only if $n = 4k+1$ for all $k \geq 1$.
4) In any dihedral group, prove that the composition of two reflections is a rotation.

13 Topics in Finite Groups

Many of the results concerning finite groups rely on the well-known Sylow theorems, some of which are stated without proof as follows.

Theorem 13.1 (Sylow's Theorem)**.** Suppose that $|G| = p^km$, where p is a prime number not dividing m. Then G has a subgroup of order p^j, for each $0 \leq j \leq k$. Moreover, the number of subgroups of order p^k is a divisor of m in the congruence class $[1]_p$ and in particular this subgroup is unique if and only if normal.

Note that Sylow's theorem supercedes that of Cauchy. We state Cauchy's theorem again next as a corollary, followed by another immediate consequence of Sylow's theorem.

Corollary 13.2 (Cauchy's Theorem)**.** Let G be a finite group of order divisible by p, a prime number. Then G has an element of order p.

Proof. It suffices if G has a subgroup of order p, because such subgroup is necessarily generated by an element of the same order. That is what Sylow's theorem says. $\triangledown$

Corollary 13.3. Let $p < q$, both prime numbers, such that $q \notin [1]_p$. Then any group of order pq is isomorphic to $\mathbb{Z}_{pq}$.

Proof. Under the given conditions, Sylow's theorem says we have a unique, hence normal, subgroups of each order p and q, call them P and Q, respectively. Let $a \in P$ and $b \in Q$. We will show that $ab = ba$. Being normal, they imply $ba^{-1}b^{-1} \in P$ and $aba^{-1} \in Q$. Now let $x = aba^{-1}b^{-1} = a(ba^{-1}b^{-1}) = (aba^{-1})b^{-1}$; the first identity says $x \in P$ and the second $x \in Q$. Hence x belongs to $P \cap Q$, a subgroup whose order divides both p and q, so it is trivial. We conclude $e = x = aba^{-1}b^{-1}$ and $ab = ba$.

Next, the map $\theta : P \times Q \to G$ such that $\theta(a, b) = ab$ is a homomorphism because, by what we have shown above, $\theta((a, b)(c, d)) = acbd = abcd = \theta(a, b)\theta(c, d)$. The kernel contains (a, b) for which $ab = e$, or $a = b^{-1}$. Again this would mean $a \in P \cap Q$ and $a = e = b$. Hence θ is one-to-one and, since G is finite, onto as well. This yields the isomorphism $G \approx P \times Q \approx \mathbb{Z}_p \times \mathbb{Z}_q \approx \mathbb{Z}_{pq}$ by the Chinese remainder theorem. $\triangledown$

Efforts have been done in order to classify all finite groups of a given order, up to isomorphism. As an additional tool, the following theorem is a useful well-known fact in finite group theory.

Theorem 13.4. Every group of order p^2, where p is prime, is abelian.

Therefore, by the fundamental theorem of finite abelian groups, a group of order p^2 must be $\mathbb{Z}_{p^2}$ (cyclic) or $\mathbb{Z}_p \times \mathbb{Z}_p$ (non-cyclic). Previously, we have seen that a group of order $2p$, if $p > 2$, is either $\mathbb{Z}_{2p}$ (abelian) or D_p (non-abelian). And before that, of course, any group of order p is cyclic and isomorphic to $\mathbb{Z}_p$.

A complete classification of all finite groups of order 15 or less is given in the following table.

n	Groups of order n, up to isomorphism
1	$\mathbb{Z}_1$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6$, S_3
7	$\mathbb{Z}_7$
8	$\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, D_4, Q_8 (see Exercise 13.1)
9	$\mathbb{Z}_9$, $\mathbb{Z}_3 \times \mathbb{Z}_3$
10	$\mathbb{Z}_{10}$, D_5
11	$\mathbb{Z}_{11}$
12	$\mathbb{Z}_{12}$, $\mathbb{Z}_6 \times \mathbb{Z}_2$, A_4, D_6, Q_{12} (see Remark below)
13	$\mathbb{Z}_{13}$
14	$\mathbb{Z}_{14}$, D_7
15	$\mathbb{Z}_{15}$

Beyond this table, there are 14 groups of order 16 and, to mention some of the extremes, 51 of order 32 and 267 of order 64.

Remark. The notation $Q_{12} = \langle a, b \mid a^4 = b^3 = a^3bab = e\rangle$ stands for the group generated by two elements a, b under the given defining relations. Note that the last identity can be written $ba = ab^2$. You can check the Cayley table for the 12 elements of $\{a^j b^k \mid 1 \leq j \leq 4,\ 1 \leq k \leq 3\}$ in order to see why this non-abelian group is neither A_4 nor D_6.

Definition. A group G is *simple* if it has no normal subgroups other than $\{e\}$ and G itself.

Simple groups are an important and difficult topic in finite group theory, and which are closely connected to the study of polynomial equations. Roughly speaking, knowing a normal subgroup H of G enables one to study the smaller factor group G/H. Therefore, identifying finite simple groups will help in the classification problem of finite groups in general.

Example. There are no simple groups of order 20. Since $20 = 4 \times 5$, by Sylow's theorem any group G of order 20 has a subgroup of order 5. The number n of such subgroups divides 4 and belongs to the congruence class $[1]_5$. Only $n = 1$ meets these conditions. Being unique, this subgroup of order 5 is normal, hence G is not simple.

We have seen in Corollary 6.5 that any group of prime order is simple and is essentially $\mathbb{Z}_p$—in fact too simple, as it has no non-trivial subgroups at all. We shall now demonstrate why there are no simple abelian groups other than these.

Theorem 13.5. Every simple abelian group is isomorphic to $\mathbb{Z}_p$ for some prime p.

Proof. For abelian groups, all subgroups are normal. So an abelian group G can be simple only if it has no proper subgroups. In particular, $\langle a\rangle = G$ for any non-identity element $a \in G$. And we know that the only cyclic groups with no proper subgroups are those of prime order. $\bigtriangledown$

It has also been proved that there are no non-abelian simple groups of odd order, nor of order twice an odd number. On the other hand, a whole class of non-abelian simple groups of even order is given by the alternating groups:

Theorem 13.6. The alternating group A_n is simple if and only if $n \geq 5$.

Exercise 13. Complete this homework set before we continue to the next section.

1) The *quaternion group* $Q_8 = \{\pm E, \pm I, \pm J, \pm K\}$ is a subgroup of $SL(2, \mathbb{C})$, where

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \quad K = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

   a) Draw the Cayley table to verify that Q_8 is indeed a subgroup of $SL(2, \mathbb{C})$.
   b) Determine the order of each element in Q_8.
   c) Draw the subgroup lattice for Q_8, noting that it has 4 non-trivial subgroups.
   d) Show that every subgroup of Q_8 is normal, despite its being non-abelian.

2) Classify all groups of order below 100 to which Corollary 13.3 can be applied.
3) Prove that there can only be two groups of order 99.
4) Prove that no simple group has order 30.

14 Rings

Definition. Let R be a set together with two binary operations, refered to as *addition* $(+)$ and *multiplication* $(\times)$. Then R is a *ring* if it has the following properties.

1) R is an abelian group under addition.

2) Multiplication in R is *associative*, meaning that $a \times (b \times c) = (a \times b) \times c$ for every $a, b, c \in R$.

3) *Distributive laws* hold in R, meaning that $a \times (b + c) = (a \times b) + (a \times c)$ and $(a + b) \times c = (a \times c) + (b \times c)$ for every $a, b, c \in R$.

Note that the first property is composed of the following four.

1) Addition in R is commutative: $a + b = b + a$ for every $a, b \in R$.

2) Addition in R is associative: $a + (b + c) = (a + b) + c$ for every $a, b, c \in R$.

3) There exists a unique identity element in R under addition—the *zero element*, which is denoted by 0, such that $a + 0 = a$ for every $a \in R$.

4) For each $a \in R$ there exists a unique inverse element—the *negative* of a, which is written $-a$, such that $a + (-a) = 0$.

Example. Let us illustrate this idea with a few examples.

1) The set $\mathbb{Z}$ of integers under ordinary addition and multiplication is a ring. The zero element is given by the integer 0 and the negative of $a \in \mathbb{Z}$ is the integer $-a$.

2) Similarly the sets $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ of rational numbers, real numbers, and complex numbers, are respectively rings under ordinary addition and multiplication.

3) The subset of even numbers is a ring on its own. More generally the set of multiples of n, that is, $\langle n \rangle = \{nk \mid k \in \mathbb{Z}\}$ is a ring under ordinary addition and multiplication.

4) The set $\mathbb{Z}_n$ of modular integers under addition and multiplication mod n is a ring. The zero element is $0 = [0]_n$ and the negative of $[a]_n$ is given by $-[a]_n = [-a]_n$.

5) The set $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ is a ring under ordinary addition and multiplication.

6) The set $M(2, \mathbb{R})$ of 2×2 matrices with real entries is a ring under matrix additon and matrix multiplication. Similar statement holds with $\mathbb{R}$ replaced by $\mathbb{Z}, \mathbb{Q}$, or $\mathbb{C}$ as well.

Remark. From now on we write ab instead of $a \times b$. Moreover, associativity implies that the sum $a + b + c$ and the product abc may be written without requiring brackets. This can be generalized to any finite number of elements, such as $a_1 a_2 \cdots a_k$.

Definition. Unlike addition, multiplication is not assumed commutative in a ring. However, if it is then the ring R is called *commutative*. And if there exists an identity element under multiplication, we shall call it *unity* and denote it by 1. Hence, a unity in R is an element $1 \in R$ satisfying $a1 = 1a = a$ for every $a \in R$.

Note that all the examples given above are commutative rings with unity, except the last one is not commutative since matrix multiplication is generally not.

Proposition 14.1. Let R be a ring. For every $a, b, c \in R$,

1) $0a = a0 = 0$

2) $a(-b) = -(ab) = (-a)b$

3) $a(b-c) = ab - ac$ and $(b-c)a = ba - ca$

4) $(-1)a = -a$ if unity exists.

Proof. Using the definition of zero and the distributive law, $a0 = a(0+0) = a0 + a0$. Adding $-(a0)$ to both sides produces $0 = a0$. Similarly we show $0a = 0$ in order to establish (1). The rest of the proof is left as an exercise. $\triangledown$

Theorem 14.2. If R and S are two rings, with their respective additions and multiplications, then the set $R \times S = \{(r,s) \mid r \in R \text{ and } s \in S\}$ is also a ring under the usual component-wise operations. We call this ring the *direct product* of R and S.

Proof. Exercise. $\triangledown$

Definition. A subset S of a ring R is a *subring* if S is itself a ring with respect to the same addition and multiplication of R.

For example, we have the tower of subrings given by $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$. Also, the even numbers form a subring of $\mathbb{Z}$. Because a subring is necessarily a subgroup with respect to addition, from group theory we know that all subrings of $\mathbb{Z}$ must come in the form $\langle n \rangle$. The next theorem can be used to show that for each $n \in \mathbb{Z}$, the subgroup $\langle n \rangle$ is indeed a subring of $\mathbb{Z}$.

Theorem 14.3. Let R be a ring. A subset $S \subseteq R$ is a subring if and only if S is a subgroup of R under addition and is closed under multiplication. (Being closed under multiplication means that $ab \in S$ whenever $a, b \in S$.)

Proof. In class. $\triangledown$

For example, we may verify that the set $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ is indeed a ring by showing that $\mathbb{Z}[\sqrt{2}]$ is a subring of $\mathbb{R}$, by means of Theorem 14.3: For all $a, b, c, d \in \mathbb{Z}$ we have (i) $(a + b\sqrt{2}) - (c + d\sqrt{2}) = (a-c) + (b-d)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ and (ii) $(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$.

Exercise 14. Complete this homework set before we continue to the next section.

1) Given the ring R, prove that $S \subseteq R$ is a subring: (a) $\{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{R}$ (b) $\left\{\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a, d \in \mathbb{Z}\right\} \subseteq M(2,\mathbb{Z})$ (c) $\left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R}\right\} \subseteq M(2,\mathbb{R})$ (d) $\{0,2,4,6,8,10\} \subseteq \mathbb{Z}_{12}$.
2) If S and T are both subrings of R, prove that $S \cap T$ is also a subring of R.
3) Let R be a ring and $a \in R$. Prove that the subset $S \subseteq R$ is a subring, where $S =$ (a) $\{x \in R \mid ax = 0\}$ (b) $\{x \in R \mid ax = xa\}$ (c) $\{x \in R \mid rx = xr \text{ for all } r \in R\}$ (d) $\{ax \mid x \in R\}$
4) Let R be a ring. Prove that if R is cyclic as a group under addition, then R is commutative as a ring.

15 Integral Domains

Definition. Let a and b be two nonzero elements in a ring R. If $ab = 0$ then a and b are each called a *zero divisor* of R.

Example. There are zero divisors in $M(2, \mathbb{R})$, e.g., $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$. You may check that AB is the zero matrix. Another example, in $\mathbb{Z}_6$ we have $3 \times 4 \equiv 0 \pmod 6$, hence 3 and 4 are zero divisors there.

Lemma 15.1. A nonzero element $m \in \mathbb{Z}_n$ is a zero divisor if and only if m and n are not relatively prime.

Proof. Suppose m and n have a common divisor $d > 1$. Then $m(n/d) \equiv 0 \pmod n$ where $1 \leq n/d < n$ is a nonzero element. Hence m is a zero divisor. Conversely if m and n are relatively prime, the relation $mb \equiv 0 \pmod n$ implies, by Euclid's lemma, that $b \equiv 0 \pmod n$. Hence m is not a zero divisor. $\triangledown$

Remark. Equivalently, the nonzero element $m \in \mathbb{Z}_n$ is not a zero divisor if and only if $m \in U_n$. In other words, the zero divisors of $\mathbb{Z}_n$ are precisely elements of the set $\mathbb{Z}_n - (U_n \cup \{0\})$.

Proposition 15.2. Let R be a ring with a nonzero element a that is not a zero divisor. For any $b, c \in R$, if $ab = ac$ then $b = c$. Similarly, $ba = ca$ implies $b = c$.

Proof. If $ab = ac$ then $0 = ab - ac = a(b - c)$ and, since a is not a zero divisor, we must have $b - c = 0$, i.e., $b = c$. $\triangledown$

Definition. A ring R is an *integral domain* if R is a commutative ring with unity and without zero divisors.

Example. The rings $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ are all integral domains.

Remark. Proposition 15.2 says that the *cancellation laws* hold in an integral domain (both right and left since commutative) because of the lack of zero divisors. In other rings cancellation laws may fail, e.g., in $\mathbb{Z}_6$ we have $2 \times 1 \equiv 2 \times 4 \pmod 6$, but cancelling the 2 results in $1 \equiv 4 \pmod 6$, which is false. The next theorem explains why $\mathbb{Z}_6$ is not an integral domain.

Theorem 15.3. The ring $\mathbb{Z}_n$ is an integral domain if and only if n is prime.

Proof. This follows from the preceding lemma since a number n is prime if and only if it is relatively prime to $1, 2, \ldots, n - 1$. $\triangledown$

Definition. Let R be a ring with unity. If $ab = 1$ in R, then a and b are each called a *unit* element. (Do not confuse a unit with unity. Perhaps we should call unit elements *unity divisors,* to go with zero divisors.)

Thus if R is commutative, then unit elements are those with a multiplicative inverse. We denote the inverse of a under multiplication by a^{-1} and reserve the term *inverse* for mutiplication, since under addition we have agreed to use the word *negative.*

Example. The units of $\mathbb{Z}_n$ form the subset U_n. (Recall, U is for *units.*) In particular, we will see that zero divisors and units are always mutually exclusive.

Theorem 15.4. Let R be a commutative ring with unity.

1) No zero divisor is a unit.

2) If $a \in R$ is a unit, then $ab = ac$ implies $b = c$.

3) The units of R form a group under multiplication.

4) If R is finite, then every nonzero element is either a unit or a zero divisor.

Proof. In class. ▽

Remark. Note that the *finite* condition in (4) is essential; For example, all the integers in the ring $\mathbb{Z}$, other than ± 1, are neither units nor zero divisors.

Definition. A ring R is a *field* if R is a commutative ring with unity in which every nonzero element is a unit. In other words, the nonzero elements of a field form an abelian group under multiplication.

Example. The rings $\mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ are all fields. But $\mathbb{Z}$ is not a field since no integer can have a multiplicative inverse except ± 1.

Theorem 15.5. A field is an integral domain.

Proof. Let F be a field and $a \in F$, nonzero. It suffices to show that a is not a zero divisor, and that is because a is a unit. ▽

Theorem 15.6. A finite integral domain is a field.

Proof. Let $R = \{a_1, a_2, \dots, a_n\}$ be an integral domain and choose $a \in R$, nonzero. It suffices to show that $ab = 1$ for some $b \in R$. The elements $aa_1, aa_2, \dots, aa_n$ are all distinct since $aa_j = aa_k$ implies $a_j = a_k$ by the cancellation law, hence they make up all the elements of R. In particular one of them is $aa_i = 1$. ▽

Corollary 15.7. The ring $\mathbb{Z}_n$ is a field if and only if n is a prime number.

Proof. Because $\mathbb{Z}_n$ is finite and is an integral domain if and only if n is prime, according to Theorem 15.3. ▽

Remark. From a different angle, we can see why $\mathbb{Z}_p$ is a field, where p is prime: because its nonzero elements make up the abelian group U_p under multiplication mod p.

Definition. Let F be a field. A subset $S \subseteq F$ is a *subfield* if S is itself a field with respect to the addition and multiplication associated with F.

Theorem 15.8. A subset S of a field F is a subfield if and only if S is a subgroup of F under addition and S^* is a subgroup of F^* under multiplication.

Proof. This follows from the subgroup test of Theorem 4.2. ▽

Remark. The notation F^* stands for the set of nonzero elements of F, and similarly for S^*. This theorem in particular implies that the zero and unity of the subfield S are the same as those of F, respectively.

Exercise 15. Complete this homework set before we continue to the next section.

1) Let R be a commutative ring with no zero divisors. Prove that if R is finite, then R is an integral domain.
2) Find all the zero divisors and units in (a) $\mathbb{Z}_{24}$ (b) $\mathbb{Z}_4 \times \mathbb{Z}_5$ (c) $\mathbb{Q} \times \mathbb{Q}$ (d) $M(2, \mathbb{R})$.
3) Show why $R \times S$ is not an integral domain, for any rings R and S.
4) Prove that the set $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ is a subfield of $\mathbb{R}$.

16 Ideals

Definition. A subset I of a ring R is an *ideal* if I is a subgroup under addition such that if $a \in I$ and $r \in R$ then $ar, ra \in I$.

By Theorem 14.3 an ideal is a subring, but it is more than just a subring. (Roughly speaking, an ideal for rings is the analogue of a normal subgroup for groups, in the sense that it is the kernel of a homomormphism.) For example, the subring $\langle n \rangle$ of $\mathbb{Z}$ is an ideal, for if a is a multiple of n then ar is still a multiple of n for any $r \in \mathbb{Z}$.

Definition. Let R be a commutative ring with unity. For every $a \in R$ define the set $(a) = \{ra \mid r \in R\}$. The next theorem demonstrates that (a) is an ideal of R, which we now call the *principal ideal* of R generated by a. Moreover, we call an ideal I *principal* if $I = (a)$ for some $a \in R$. (Compare a principal ideal to a cyclic subgroup, where it is generated by one element.)

Theorem 16.1. Let R be a commutative ring with unity. For every $a \in R$, the set $(a) = \{ra \mid r \in R\}$ is an ideal.

Proof. If $r, s \in R$, the fact that $ra - sa = (r - s)a$ shows that (a) is a subgroup under addition. Moreover, given $ra \in (a)$ and $s \in R$, we have $s(ra) = (sr)a \in (a)$. $\bigtriangledown$

Remark. Note that the ideal $\langle n \rangle$ of $\mathbb{Z}$ is really the principal ideal $\langle n \rangle = (n)$. For this reason, we loosely refer to the elements of (a) as *multiples* of a in R.

Recall that every subgroup of a cyclic group is cyclic. The next definition is the ring analogue of this property, which still holds in $\mathbb{Z}$.

Definition. A ring R is a *principal ideal domain* if R is an integral domain in which every ideal is principal.

Theorem 16.2. The ring $\mathbb{Z}$ is a principal ideal domain.

Proof. $\mathbb{Z}$ is integral domain where all ideals (subgroups) are of the form $\langle n \rangle = (n)$. $\bigtriangledown$

Theorem 16.3. Let F be a field. The only ideals of F are $\{0\}$ and F itself. Conversely, let R be a commutative ring with unity and no ideals other than $\{0\}$ and R itself. Then R is a field.

Proof. Let I be an ideal of F. Suppose there is $a \in I$, nonzero. Since $a^{-1} \in F$, being an ideal implies $a^{-1}a = 1 \in I$. Then $1r = r \in I$ for all $r \in F$. Hence $I = F$. Now let $a \in R$, nonzero. Then by hypothesis, $(a) = R$ and, in particular, $1 = ra$ for some $r \in R$. Hence a is a unit and R is a field. $\bigtriangledown$

Remark. As a result, although trivial, we see that all fields are principal ideal domains since their only ideals are (0) and (1).

Exercise 16. Complete this homework set before we continue to the next section.

1) Let $S = \{(n, n) \mid n \in \mathbb{Z}\}$. Prove that S is a subring of $\mathbb{Z} \times \mathbb{Z}$ which is not an ideal.
2) Let R be a ring, not necessarily commutative, and let I denote an ideal in R. Prove that the set S is also an ideal of R, where (a) $S = \{r \in R \mid ra = 0 \text{ for all } a \in I\}$ (b) $S = \{r \in R \mid ra \in I \text{ for all } a \in R\}$.
3) For I, J ideals of a ring R, we define $I + J = \{a + b \mid a \in I, b \in J\}$. (a) Prove that $I + J$ is an ideal of R, and (b) show that $(m) + (n) = (\gcd(m, n))$ as ideals of $\mathbb{Z}$.
4) Prove that the principal ideal (2) in $\mathbb{Z}_{10}$ is a field.

17 Factor Rings

Let I be a subring of a ring R. Since R is an abelian group, under addition, then I is a normal subgroup of R. Hence we have the factor group of cosets, $R/I = \{I{+}r \mid r \in R\}$, in which $(I{+}r)+(I{+}s) = I+(r{+}s)$. We now wish to make R/I a ring by introducing the multiplication $(I+r)(I+s) = I+rs$. This will work, however, only if I is an ideal.

Lemma 17.1. Let I be an ideal of a ring R. For every elements $I+r$ and $I+s$ in the factor group R/I, the multiplication $(I+r)(I+s) = I+rs$ is well defined.

Proof. Suppose that $I+r = I+r'$ and $I+s = I+s'$, hence $r-r' \in I$ and $s-s' \in I$. It follows that the multiples $rs - r's$ and $r's - r's'$ belong to I as well. Add these two elements and $rs - r's' \in I$, so $I+rs = I+r's'$. ▽

Theorem 17.2. Let I be an ideal of a ring R. The factor group R/I is a ring.

Proof. It is left to show associativity and the distributive laws. These are trivial as these properties are simply inherited from those of R. ▽

Definition. Let I be an ideal of R. The ring $R/I = \{I+r \mid r \in R\}$ is called the *factor ring* or *quotient ring* of R *mod* I.

Example. We have the old example of $\mathbb{Z}$ and the ideal (n). The factor group $\mathbb{Z}/(n) \approx \mathbb{Z}_n$ is now a ring with addition and multiplication mod n, but we already know that.

Exercise 17. Complete this homework set before we continue to the next section.

1) Construct the multiplication table for the factor ring (a) $\mathbb{Z}_{10}/(5)$ (b) $\mathbb{Z}_{12}/(9)$ (c) $2\mathbb{Z}/(6)$ (d) $\mathbb{Z}_4 \times \mathbb{Z}_6/((2,2))$ and find all the units and zero divisors in each one.
2) Prove the following claim concerning the factor ring R/I.
   a) If R is commutative with unity, then R/I is also commutative with unity.
   b) If K is an ideal of R/I, then $L = \{r \in R \mid I+r \in K\}$ is an ideal of R.
   c) If R is a principal ideal domain, then every ideal in R/I is principal.
   d) Find an example where R is a principal ideal domain but R/I is not.
3) Let R be a commutative ring with unity. A *prime* ideal $I \subset R$ has the property that for all $a, b \in R$, if $ab \in I$ then either $a \in I$ or $b \in I$. Prove that the ideal I is prime if and only if R/I is an integral domain. (In particular, the ideal $(n) \subset \mathbb{Z}$ is prime if and only if the integer n is prime.)
4) Let R be a commutative ring with unity. A *maximal* ideal $I \subset R$ has the property that for all ideals $J \subseteq R$, if $I \subseteq J$ then either $I = J$ or $J = R$. Prove that the ideal I is maximal if and only if R/I is a field.

18 Ring Homomorphisms

Definition. Let R and R' be two rings, each with their own addition and multiplication. A function $\theta : R \to R'$ is called a (ring) *homomorphism* if for every $a, b \in R$, we have $\theta(a+b) = \theta(a) + \theta(b)$ and $\theta(ab) = \theta(a)\theta(b)$.

If θ is a homomorphism, we also define the *range* of θ to be $\theta(R) = \{\theta(a) \mid a \in R\}$ and the *kernel* $\ker(\theta) = \{a \in R \mid \theta(a) = 0\}$. Both the zero elements for R and for R' are denoted by 0, but they should be distinguishable from the context.

Example. Let $\theta : \mathbb{Z} \to \mathbb{Z}_n$ be given by $\theta(a) = [a]_n$. This is the familiar group homomorphism, under addition, where $\ker(\theta) = (n)$ and $\theta(\mathbb{Z}) = \mathbb{Z}_n$. Now since $[ab]_n = [a]_n[b]_n$, this θ is now a ring homomorphism.

Example. Let $R = \{a+b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ and $\theta : R \to R$, where $\theta(a+b\sqrt{2}) = a - b\sqrt{2}$. It is not hard to show that θ is a homomorphism, and that $\theta(R) = R$ and $\ker(\theta) = \{0\}$.

Proposition 18.1. Let $\theta : R \to R'$ be a ring homomorphism. Then

1) $\theta(0) = 0$ and $\theta(-a) = -\theta(a)$ for every $a \in R$.

2) θ is one-to-one if and only if $\ker(\theta) = \{0\}$.

3) $\theta(R)$ is a subring of R'.

4) $\ker(\theta)$ is an ideal of R.

Proof. In class. $\triangledown$

Definition. A ring homomorphism $\theta : R \to R'$ is called an *isomorphism* if θ is one-to-one and onto, in which case we say that R and R' are *isomorphic*, written $R \approx R'$.

Like the isomorphism between two groups, a ring isomorphism preserves the structure of the one ring onto the other, with respect to both addition and multiplication. Thus two isomorphic rings are essentially the same ring except for the different labelling of the elements. In particular if $R \approx R'$, then R is an integral domain, or a field, if and only if R' is an integral domain or a field, respectively.

Theorem 18.2 (The Fundamental Homomorphism Theorem for Rings)**.** Suppose that $\theta : R \to R'$ is a homomorphism of rings. Then $R/\ker(\theta) \approx \theta(R)$.

Proof. Let $I = \ker(\theta)$ and $\Theta(I + r) = \theta(r)$. We have seen that $\Theta : R/I \to \theta(R)$ is a group isomorphism under addition. It is left to show that Θ preserves multiplication: $\Theta((I + r)(I + s)) = \Theta(I + rs) = \theta(rs) = \theta(r)\theta(s) = \Theta(I + r)\Theta(I + s)$. $\triangledown$

Example. From the previous example we now have $\mathbb{Z}/(n) \approx \mathbb{Z}_n$ as rings.

Theorem 18.3 (Chinese Remainder Theorem for Rings)**.** Suppose that m and n are relatively prime positive integers. Then $\mathbb{Z}_m \times \mathbb{Z}_n \approx \mathbb{Z}_{mn}$ (as rings).

Proof. Recall the homomorphism $\theta : \mathbb{Z} \to \mathbb{Z}_m \times \mathbb{Z}_n$, as additive groups, given by $\theta(a) = ([a]_m, [a]_n)$. This map is onto with $\ker(\theta) = (mn)$. The fundamental theorem gives the claim since $\theta(ab) = \theta(a)\theta(b)$, showing that θ is a ring homomorphism. $\triangledown$

Exercise 18. Complete this homework set before we continue to the next section.

1) Let $\theta : \mathbb{Z}_{10} \to \mathbb{Z}_{10}$ be given by $\theta(n) =$ (a) $-n$ (b) $3n$ (c) n^2 (d) n^3. For each one, determine if θ is a group or ring isomorphism, or neither, and why.
2) Prove that $2\mathbb{Z} \approx 3\mathbb{Z}$ as groups but not as rings.
3) Let $\theta : R \to R'$ be a ring homomorphism.
   a) If θ is onto, prove that $\theta(1) = 1$, if there is unity.
   b) Give a counter-example where θ is not onto and $\theta(1) \neq 1$.
   c) If $R = R' = \mathbb{Z}_n$, prove that θ is isomorphism if and only if θ is the identity map.
   d) If R is a field, prove that either θ is one-to-one or else $\theta(a) = 0$ for all $a \in R$.
4) Prove that the subring $\left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\} \subseteq M(2, \mathbb{R})$ is isomorphic to $\mathbb{C}$, hence it is a field.

19 Polynomial Rings

Definition. Let $R[x] = \{a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots + a_nx^n \mid a_i \in R\}$, where R is a commutative ring. Every element $f \in R[x]$ is a *polynomial* with coefficients in R. For each polynomial f we define its *degree*, written $\deg f$, to be the largest integer k for which $a_k \neq 0$. The *zero polynomial*, $f = 0$, has an infinite degree, and we write $\deg f = \infty$.

Note that $R \subseteq R[x]$. We call every polynomial $f \in R$ a *constant*. In other words, a nonzero polynomial f is a constant if and only if $\deg f = 0$.

We define addition and multiplication of polynomials the usual way. If $f = \sum a_ix^i$ and $g = \sum b_ix^i$ are nonzero polynomials, then

$$\begin{aligned} f + g &= \sum_{i=0}^{M} (a_i + b_i)x^i \\ f\,g &= \sum_{i=0}^{N} c_i\,x^i \quad \text{where} \quad c_k = \sum_{i=0}^{k} a_i\,b_{k-i} \end{aligned}$$

where $M = \max\{\deg f, \deg g\}$ and $N = \deg f + \deg g$.

Theorem 19.1. If R is a commutative ring, so is $R[x]$, which we call *the ring of polynomials over R.* The zero element in $R[x]$ is the zero polynomial $f = 0$, and for each polynomial $f = \sum a_ix^i$, the negative of f is given by $-f = \sum(-a_i)x^i$.

Proof. In class. ▽

Proposition 19.2. If R is an integral domain, then $\deg fg = \deg f + \deg g$ for all nonzero polynomials $f, g \in R[x]$.

Proof. Let $\deg f = n$ and $\deg g = m$. By the rule of multiplication, it is clear that $\deg fg \leq m + n$. Also, keeping the notation above, the coefficient of x^{m+n} in fg is given by $c_{m+n} = a_nb_m$. Since $a_n, b_m \neq 0$ and R has no zero divisors, then $c_{m+n} \neq 0$. Hence $\deg fg = m + n$. ▽

Remark. In a ring other than integral domain, Proposition 19.2 may fail. For example, in $\mathbb{Z}_6[x]$ we have $(2x - 1)(3x + 2) = x - 2$ and also $4x^5 \times 3x^2 = 0$.

Corollary 19.3. If R is an integral domain, then $\deg fg \geq \deg f$ for all $f, g \in R[x]$.

Proof. This follows since the degree of any polynomial is a non-negative number. ▽

Proposition 19.4. If R is an integral domain, so is $R[x]$.

Proof. $R[x]$ is commutative with unity 1, the unity of R. And if f and g are nonzero polynomials then $fg \neq 0$ because Proposition 19.2 asserts that fg has a finite degree, unlike the zero polynomial. ▽

Exercise 19. Complete this homework set before we continue to the next section.

1) Let R be a ring. (a) Show why $R[x]$ is not a field. (b) What are the units in $R[x]$?
2) Let R be an integral domain, and let $I = \{f \in R[x] \mid f(0) = 0\}$, where $f(0)$ denotes the polynomial $f(x)$ evaluated at $x = 0$. Prove that I is a principal ideal of $R[x]$.
3) Let $I = \{f(x) \in \mathbb{Z}[x] \mid f(0) \in 2\mathbb{Z}\}$. Prove that I is an ideal of $\mathbb{Z}[x]$ which is not principal. Hence $\mathbb{Z}[x]$ is not a principal ideal domain.
4) Let $S = \{f(x) \in \mathbb{R}[x] \mid f'(0) = 0\}$, where $f'(0)$ denotes the first derivative of $f(x)$, as defined in Calculus, evaluated at 0. Prove that S is a subring of $\mathbb{R}[x]$ which is not an ideal.

20 Divisibility in $F[x]$

We consider polynomials whose coefficients lie in a field F. The integral domain $F[x]$ shares many arithmetical properties enjoyed by the ring $\mathbb{Z}$ of integers.

Definition. Let F be a field and $f, g \in F[x]$. We say that f *divides* g if $g = hf$ for some $h \in F[x]$. In this case we may also say that g is *divisible* by f, or that g is a *multiple* of f, and write $f \mid g$. Moreover, f is called a *divisor* or *factor* of g.

Example. Over the field $\mathbb{Q}$, $(x-1) \mid (\frac{1}{2}x^2+x-\frac{3}{2})$ because $(x-1)(\frac{1}{2}x+\frac{3}{2}) = \frac{1}{2}x^2+x-\frac{3}{2}$.

Proposition 20.1. In $F[x]$ the following statements hold, where F is a field.

1) The constant 1 divides all other polynomials.

2) If $f \mid g \neq 0$ then $\deg f \leq \deg g$.

3) If $f \mid g$ and $g \mid h$ then $f \mid h$.

4) If $f \mid g$ and $f \mid h$ then $f \mid ag + bh$ for all $a, b \in F[x]$.

Proof. In class. $\bigtriangledown$

Corollary 20.2. If $f \mid g$ and $g \mid f$, then $g = af$ for some constant $a \in F$.

Proof. We have $\deg f \leq \deg g \leq \deg f$, hence $\deg f = \deg g$. It follows that $g = af$ with $\deg a = 0$. $\bigtriangledown$

Theorem 20.3 (The Division Algorithm in $F[x]$)**.** Let f and g be two nonzero polynomials over a field F. Then there exist unique polynomials $q, r \in F[x]$ such that $g = qf + r$, where either $r = 0$ or $\deg r < \deg f$.

Proof. If $g = 0$ then let $q = r = 0$. If $\deg g < \deg f$ then we let $q = 0$ and $r = g$. Else, let $f = \sum_0^n a_i x^i$ and $g = \sum_0^m b_i x^i$ with $m \geq n$. By way of induction we assume the theorem is true for all g of degree less than m. Let $g' = g - cfx^{m-n}$ where $c = b_m(a_n)^{-1}$. Then either $g' = 0$ or else $\deg g' < \deg g$. By induction hypothesis, we have $g' = q'f + r$ where $r = 0$ or $\deg r < \deg f$. It follows that $g = qf + r$ with $q = q'cx^{m-n}$.

To prove uniqueness, suppose that $g = qf + r = Qf + R$ where also $R = 0$ or $\deg R < \deg f$. Then $(q-Q)f = R - r$. If $R - r \neq 0$ then $\deg(R-r) < \deg f$, whereas $\deg(q-Q)f \geq \deg f$ by Corollary 19.3. To avoid contradiction we must have $R = r$ and $(q-Q)f = 0$, which implies $q = Q$ since $F[x]$ has no zero divisors. $\bigtriangledown$

Definition. The polynomials q, r in the preceding theorem are called the *quotient* and *remainder,* respectively, upon dividing g by f. In particular, we define $g \bmod f = r$.

Corollary 20.4. [Remainder Theorem] Let $a \in F$ and $g \in F[x]$. Then $g \bmod (x-a) = g(a)$, i.e., $g(a)$ is the remainder when g is divided by $x - a$. In particular, $(x - a) \mid g$ if and only if $g(a) = 0$.

Proof. Divide g by $x - a$, and $g(x) = q(x-a) + r$. Then $g(a) = r$, the remainder. $\bigtriangledown$

Theorem 20.5. Where F is a field, the ring $F[x]$ is a principal ideal domain.

Proof. Let I be an ideal of $F[x]$ and let f be a polynomial of least degree in I. By the division algorithm, for each $g \in I$ there are $q, r \in F[x]$ such that $g = qf + r$ with either $r = 0$ or $\deg r < \deg f$. But since I is an ideal, $r = g - qf \in I$, so $\deg r < \deg f$ is not possible. Hence $r = 0$ and $g \in (f)$. We have proved that $I = (f)$. ▽

Lemma 20.6. Let $f, g \in F[x]$. The set $\{af + bg \mid a, b \in F[x]\}$ is an ideal of $F[x]$.

Proof. Exercise. ▽

Definition. Let F be a field and $f, g \in F[x]$. A *greatest common divisor* of f and g is a polynomial $d \in F[x]$ such that $(d) = \{af + bg \mid a, b \in F[x]\}$.

Proposition 20.7. Let d be a greatest common divisor of f and g in $F[x]$. Then

1) $d \mid f$ and $d \mid g$

2) $d = af + bg$ for some $a, b \in F[x]$

3) if $c \mid f$ and $c \mid g$ then $c \mid d$

4) if c is another greatest common divisor of f and g, then $c = ad$ for some $a \in F$.

Proof. In class. ▽

Definition. If $f = \sum a_i x^i \in F[x]$ with degree n, we call a_n the *leading coefficient* of f. A polynomial $f \in F[x]$ is *monic* when its leading coefficient is 1, the unity of F.

It is now clear that if $(c) = (d)$ as ideals in $F[x]$, then $c = ad$ for some constant $a \in F$. In particular, if both c and d are monic polynomials, then $a = 1$ and $c = d$. This fact enables us to define $\gcd(f, g)$ as follows.

Definition. Let F be a field and $f, g \in F[x]$. Define $\gcd(f, g) = d$, where $d \in F[x]$ is the monic polynomial for which $(d) = \{af + bg \mid a, b \in F[x]\}$. We call $\gcd(f, g)$ *the* greatest common divisor of f and g.

Theorem 20.8. For all $f, g \in F[x]$, we have $\gcd(f, g) = \gcd(g, f \bmod g)$.

Proof. In class. ▽

Example. We find that $\gcd(x^{81} - 1,\, x^{24} - 1) = x^3 - 1$ (monic) in $\mathbb{Q}[x]$ as follows.

$$\begin{aligned}(x^{81} - 1) \bmod (x^{24} - 1) &= x^9 - 1\\ (x^{24} - 1) \bmod (x^9 - 1) &= x^6 - 1\\ (x^9 - 1) \bmod (x^6 - 1) &= x^3 - 1\\ (x^6 - 1) \bmod (x^3 - 1) &= 0\end{aligned}$$

Similarly, over $\mathbb{Z}_5$ we check that $\gcd(3x^6 - x^2 + 2, 3x^4 - 2x^2 - 1) = x^2 + 2$.

Exercise 20. Complete this homework set before we continue to the next section.

1) Let F be a field and $f \in F[x]$ with $\deg f = n$. (a) Prove that f has at most n zeros over F, and (b) find a counter-example for (a) if F is not a field.
2) Find (a) $\gcd(x^{108} - 1, x^{66} - 1) \in \mathbb{Q}[x]$ (b) $\gcd(x^{14} + x^8 + x^4 + x^2 + 1, x^{12} + x^4 + 1) \in \mathbb{Z}_2[x]$ (c) $\gcd(2x^{11} + 3, 3x^7 + 2) \in \mathbb{Z}_5[x]$ (d) $\gcd(6x^5 + 2x^3 + 2x^2 + 3, 4x^4 + 5) \in \mathbb{Z}_7[x]$.
3) Let $f, g, h \in F[x]$ with $\gcd(f, g) = 1$. Prove that if $f \mid h$ and $g \mid h$, then $fg \mid h$.
4) Suppose the field F is finite with n elements. Prove each claim in the given order:

   a) $a^n = a$ for all $a \in F$.
   b) $x^n - x = \prod (x - a)$, where the product ranges over all $a \in F$.
   c) $-1 = \prod a$, where the product ranges over all $a \in F^*$.
   d) $(p - 1)! \equiv -1 \pmod{p}$, where p is prime. (Wilson's Theorem)

21 Irreducible Polynomials

Definition. Let F be a field. A polynomial $f \in F[x]$ is *reducible* if f is divisible by another polynomial $g \in F[x]$ with $0 < \deg g < \deg f$. We call f *irreducible* when f is not reducible.

Theorem 21.1. If $f \mid gh$ and f is irreducible, then $f \mid g$ or $f \mid h$.

Proof. Let $d \mid f$. If $\deg d > 0$ then $\deg d = \deg f$, and $d = af$ for some $a \in F$. If $d \mid g$ as well then $f \mid g$. Hence, if $f \nmid g$ then d is a constant, in which case $\gcd(f, g) = 1$. We then write $1 = af + bg$. Multiply by h to get $h = afh + bgh$. Since f divides the right hand side then $f \mid h$. $\triangledown$

Theorem 21.2 (Unique Factorization in F[x])**.** Over a field, every non-constant monic polynomial is the product of a unique collection of irreducible monic polynomials, counting repetition.

Proof. In class. $\triangledown$

Theorem 21.3. Let F be a field and $f \in F[x]$. Then f is irreducible if and only if the factor ring $F[x]/(f)$ is a field.

Proof. Let $R = F[x]/(f)$. If f is reducible then $f = gh$ in $F[x]$, where f divides neither g nor h. It follows that $(f) + g$ and $(f) + h$ are two nonzero elements in R whose product is $((f)+g)((f)+h) = (f)+f = 0$. This shows that R is not an integral domain, nor a field.

Conversely, let f be irreducible and $(f) + c \in R$ be a nonzero element. Since $f \nmid c$ then $\gcd(f, c) = 1$. By Proposition 20.7 there exist $a, b \in F[x]$ such that $af + bc = 1$. Therefore $((f) + b)((f) + c) = (f) + 1 - af = (f) + 1$, the unity in R. This shows that $(f) + c$ is a unit element, hence R is a field. $\triangledown$

Example. The polynomial $f(x) = x^2 + 1 \in \mathbb{R}[x]$ is irreducible since f has no real zero, hence $\mathbb{R}[x]/(x^2 + 1)$ is a field. What are its elements? Using division algorithm every $g \in \mathbb{R}[x]$ can be written $g = q(x^2 + 1) + r$ with $r = 0$ or $\deg r \leq 1$. Hence $\mathbb{R}[x]/(x^2 + 1) = \{(x^2 + 1) + a + bx \mid a, b \in \mathbb{R}\}$. Since $x^2 + 1 = 0$ in this factor ring, we can show that $\mathbb{R}[x]/(x^2 + 1) \approx \{a + bi \mid a, b \in \mathbb{R},\ i^2 = -1\} = \mathbb{C}$. In a similar way, we can see that the factor ring $\mathbb{Q}[x]/(x^2 - 2)$ is actually the field $\mathbb{Q}[\sqrt{2}]$ of Exercise 15.4.

Theorem 21.4. Let F be a field and $f \in F[x]$ with $\deg f = 2$ or 3. Then f is reducible if and only if f has a zero in F.

Proof. If we factor $f = gh$, then either g or h must be linear, say $g = ax + b$, implying that $-ba^{-1}$ is a zero of f. Conversely, if $f(a) = 0$, then $x - a$ is a factor of f by Corollary 20.4, regardless of $\deg f$. $\triangledown$

Example. The polynomial $x^2 + 1$ has no zero over $\mathbb{Z}_7$ but has two zeros over $\mathbb{Z}_5$, i.e., 2 and 3. So it is irreducible in $\mathbb{Z}_7[x]$ and reducible in $\mathbb{Z}_5[x]$, where $x^2+1 = (x-2)(x-3)$. Similarly, the existence or non-existence of a zero will prove that x^3+x+1 is irreducible over $\mathbb{Z}_5$ and $\mathbb{Z}_7$ but reducible over $\mathbb{Z}_{11}$ and $\mathbb{Z}_{13}$.

Remark. The preceding result does not hold for higher degree polynomials. For instance, $f = (x^2 + 1)(x^2 + 1) \in \mathbb{Q}[x]$ is obviously reducible without any rational zero.

Definition. The polynomial $f \in \mathbb{Z}[x]$ is *primitive* if $f \neq ag$ for any integer $a \geq 2$ and $g \in \mathbb{Z}[x]$. In particular, a monic polynomial is always primitive.

Lemma 21.5. If f and g are primitive then fg is also primitive.

Proof. Let $f = \sum a_i x^i$, $g = \sum b_i x^i$ and $fg = \sum c_i x^i$. By way of contradiction suppose there is a prime $p \mid c_i$ for all i. Since f is primitive, not all its coefficients are divisible by p. Let j be the smallest such that $p \nmid a_j$. Similarly k is the smallest such that $p \nmid b_k$. Since $p \mid c_{j+k} = \sum_{i=0}^{j+k} a_i\, b_{j+k-i}$ then $p \mid a_j b_k$, contradicting Euclid's lemma. $\triangledown$

Theorem 21.6 (Gauss' Lemma)**.** Suppose that $f \in \mathbb{Z}[x]$ is primitive. If f is reducible over $\mathbb{Q}$, then f can be properly factored in $\mathbb{Z}[x]$.

Proof. Let $f = gh \in \mathbb{Q}[x]$. Using least common denominator we can find $a \in \mathbb{Q}$ such that $ag \in \mathbb{Z}[x]$ and is primitive. Similarly, $bh \in \mathbb{Z}[x]$ for some $b \in \mathbb{Q}$. Then the product $agbh = abf \in \mathbb{Z}[x]$ is primitive, and so $ab = 1$. Thus we factor $f = (ag)(bh)$ in $\mathbb{Z}[x]$. $\triangledown$

Example. Suppose we know that $6x^2 + x - 2 = (3x - \frac{3}{2})(2x + \frac{4}{3}) \in \mathbb{Q}[x]$. Then we can write $6x^2 + x - 2 = \frac{3}{2}(2x - 1)\frac{2}{3}(3x + 2) = (2x - 1)(3x + 2) \in \mathbb{Z}[x]$.

Theorem 21.7 (Eisenstein's Criterion)**.** Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$. If there is a prime number p such that $p^2 \nmid a_0$, $p \mid a_0$, $p \mid a_1$, $\ldots$, $p \mid a_{n-1}$, but $p \nmid a_n$, then f is irreducible in $\mathbb{Q}[x]$.

Proof. We assume f is primitive, otherwise factor out the gcd without affecting the proof. By contradiction suppose f can be factored in $\mathbb{Q}[x]$. Then by Gauss' lemma we may write $f(x) = (b_0 + b_1 x + \cdots b_r x^r)(c_0 + c_1 x + \cdots c_s x^s)$ with integer coefficients, $r, s \geq 1$. Since $p \mid a_0 = b_0 c_0$ then $p \mid b_0$ or $p \mid c_0$ but not both since $p^2 \nmid a_0$. Assume $p \mid b_0$ and $p \nmid c_0$. Since f is primitive, let $k < r$ be the least such that $p \nmid b_k$. But $p \mid a_k = b_0 c_k + b_1 c_{k-1} + \cdots + b_k c_0$ hence $p \mid b_k c_0$—impossible since $p \nmid b_k$ and $p \nmid c_0$. $\triangledown$

Example. The polynomial $x^5 + 6x^3 - 12$ is irreducible over $\mathbb{Q}$ because the theorem applies with $p = 3$ (but not $p = 2$). Similarly, any polynomial of the form $x^n \pm p$ is irreducible over $\mathbb{Q}$, if p is a prime number.

Theorem 21.8. Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$. Suppose that p is a prime such that $p \nmid a_n$. Taking mod p of the coefficients, if f is irreducible in $\mathbb{Z}_p[x]$ then f is irreducible in $\mathbb{Q}[x]$.

Proof. By contrapositive, assume that $f = gh \in \mathbb{Q}[x]$ with $\deg g, \deg h < \deg f$. Since $\deg f$ is unchanged when viewed mod p, then the inequality $\deg g, \deg h < \deg f$ also holds in $\mathbb{Z}_p[x]$. So f is reducible over $\mathbb{Z}_p$. $\triangledown$

Example. Let $f = 3x^3 - x^2 + 2x + 7 \in \mathbb{Q}[x]$, which corresponds to $x^3 - x^2 + 1 \in \mathbb{Z}_2[x]$. The latter is irreducible in $\mathbb{Z}_2[x]$ (why?) so f is also irreducible over $\mathbb{Q}$.

Remark. The converse is false, e.g., $x^2 + 1$ is irreducible over $\mathbb{Q}$ and reducible over $\mathbb{Z}_2$.

Exercise 21. Complete this homework set before we continue to the next section.

1) Factor $f = x^3 + 1$ and $g = 3x^4 + 5x^2 - 1$ using irreducible polynomials over the field (a) $\mathbb{Z}_2$ (b) $\mathbb{Z}_7$ (c) $\mathbb{Z}_{11}$ (d) $\mathbb{R}$.
2) Prove irreducible: (a) $2x^3 + x + 6 \in \mathbb{Q}[x]$ (b) $x^4 + x + 1 \in \mathbb{Z}_2[x]$ (c) $x^4 + 1 \in \mathbb{Q}[x]$ (Hint: substitute $x = t + 1$ into Theorem 21.7) (d) $3x^4 - 6x^3 + 2x^2 - x + 7 \in \mathbb{Q}[x]$.
3) Let $f = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$. (a) Prove that if $f(a/b) = 0$ for some $a, b \in \mathbb{Z}$ with $\gcd(a, b) = 1$, then $a \mid a_0$ and $b \mid a_n$. (Hence, if f is monic, then any rational zero must be an integer.) (b) Use this to factor $2x^4 + 3x^3 - 2x^2 - x + 3$ over $\mathbb{Z}$.
4) Find all the irreducible polynomials in $\mathbb{Z}_2[x]$ of degree (a) 2 (b) 3 (c) 4 (d) 5.

22 Field Extensions

Definition. When we have a field K and a subfield F, we say that K is an *extension field* over F.

Lemma 22.1. Let K be an extension field over F, and fix an element $a \in K$. Then the set $\{g \in F[x] \mid g(a) = 0\}$ is an ideal of $F[x]$.

Proof. In class. $\triangledown$

Definition. Let $a \in K$, an extension field over F. In view of the fact that $F[x]$ is a principal ideal domain, we define the *minimal polynomial* of a over F to be the monic polynomial $f \in F[x]$ such that $(f) = \{g \in F[x] \mid g(a) = 0\}$. We will assume only the case where $a \in K$ is *algebraic* over F, i.e., when its minimal polynomial is nonzero.

Theorem 22.2. Let $a \in K$ be algebraic over F. Then $f \in F[x]$ is the minimal polynomial of a over F if and only if f is monic, irreducible, and $f(a) = 0$. Moreover with such f, if $g(a) = 0$ for any $g \in F[x]$ then $f \mid g$ and in particular $\deg f \leq \deg g$.

Proof. Let f be the minimal polynomial; it is clear that f is monic and $f(a) = 0$. Then if we factor $f = gh$, either $g(a) = 0$ or $h(a) = 0$. If say, $g(a) = 0$, then $g \in (f)$ and $f \mid g$, which is not so if g is a proper factor of f. Hence f is irreducible. Conversely, let $f_2 \in F[x]$ with $f_2(a) = 0$. Then $f \mid f_2$, so if f_2 is irreducible then f_2 must be a constant multiple of f. If f_2 is also monic, then $f_2 = f$. $\triangledown$

Remark. For such f, whenever $g(a) = 0$ we have $f \mid g$ and $\deg f \leq \deg g$. Hence f is minimal in the sense that its degree is least possible under the condition that $f(a) = 0$. Note that $\deg f = n$ if and only if n is the smallest exponent such that $a^n \in K$ can be written as a linear combination of $1, a, a^2, \ldots, a^{n-1}$ using coefficients from F.

Example. Both $\sqrt{2} \in \mathbb{R}$ and $i \in \mathbb{C}$ are algebraic elements over $\mathbb{Q}$ with minimal polynomials $x^2 - 2$ and $x^2 + 1$, respectively. Applying the above remark, we can check that $x^4 - 10x^2 + 1$ is the minimal polynomial of $\sqrt{2} + \sqrt{3}$ (hence irreducible) over $\mathbb{Q}$.

Definition. Let $F \subseteq K$ be a field extension, and consider a subset $S \subseteq K$. We define $F(S)$ to be the smallest field containing S, such that $F \subseteq F(S) \subseteq K$. In particular, when $S = \{a_1, \ldots, a_k\}$, we shall simply write $F(a_1 \ldots, a_k)$ instead of $F(S)$.

Example. Consider $\mathbb{Q}(\sqrt{2})$. Being a field, $\mathbb{Q}(\sqrt{2}) \supseteq \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. The latter we know is a field, hence $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$.

Theorem 22.3. Let $a \in K$ be an algebraic element over F with minimal polynomial $f \in F[x]$. Then $F(a) \approx F[x]/(f)$.

Proof. The idea is to define the homomorphism $\theta : F[x] \to F(a)$ by $\theta(g(x)) = g(a)$ and show that $\ker(\theta) = (f)$, then apply the fundamental homomorphism theorem. $\triangledown$

Corollary 22.4. Suppose that $a, b \in K$ have the same minimal polynomial f over F. Then $F(a) \approx F(b)$.

Proof. Both fields are isomorphic to $F[x]/(f)$ by Theorem 22.3. $\triangledown$

Remark. To clarify some terminology, we say that a is a *zero* of a polynomial f when we mean that $f(a) = 0$. Meanwhile, the term *root* refers to a solution of a polynomial equation. Hence, a is a zero of f if and only if a is a root of $f(x) = 0$. Of course, do distinguish a zero of a polynomial from the zero element of a ring.

Theorem 22.5. Every non-constant polynomial $f \in F[x]$ has a zero in some extension field K over F.

Proof. We assume that f is irreducible for if $g(a) = 0$ for some factor g then $f(a) = 0$ too. Then $K = F[x]/(f)$ is a field. Now let $\theta : F \to K$ with $\theta(c) = (f) + c$. We see that θ is a one-to-one homomorphism, so $F \approx \theta(F)$, a subfield of K. Essentially the element $a = (f) + x \in K$ is a zero of f as $f(a) = (f) + f(x) = (f)$, the zero of K. $\triangledown$

Corollary 22.6. For every $f \in F[x]$ there is an extension field K over F such that $f = a\prod(x - a_i) \in K[x]$.

Proof. By the theorem f is divisible by $(x - a)$, where a belongs to some extension field over F. The proof is done by induction on the degree of f. $\triangledown$

Definition. We say that a polynomial $f \in F[x]$ *splits* in some extension wherein $f = a\prod(x - a_i)$. The field $F(a_1, \dots, a_n)$ is called a *splitting field* for f over F. It can be shown that any two splitting fields for the same polynomial are isomorphic.

Example. A splitting field for $x^2 + 1$ over $\mathbb{Q}$ is $\mathbb{Q}(\pm i) = \mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$. Over $\mathbb{R}$, the same polynomial has splitting field $\mathbb{C}$.

The field $\mathbb{C}$ of complex numbers has the property that every $f \in \mathbb{C}[x]$ splits without the need of an extension field. Such a field is called *algebraically closed.* We state the big theorem without a proof, which is usually provided in a complex analysis text.

Theorem 22.7 (The Fundamental Theorem of Algebra)**.** Let $f \in \mathbb{C}[x]$ have degree n. Then f has n complex zeros, counting multiplicity.

Definition. If $(x - a)^2 \mid f$ in its splitting field, we say that a is a *multiple zero* of f.

In order to classify multiple zeros, the next theorem borrows from Calculus the term *derivative* of $f = \sum a_k x^k \in F[x]$, i.e., $f' = \sum k a_k x^{k-1} \in F[x]$, where the integer k is translated as the element $k := \sum_{j=1}^{j=k} 1 \in F$.

Lemma 22.8. For every $f, g \in F[x]$ we have $(f + g)' = f' + g'$ and $(fg)' = f'g + fg'$.

Proof. Exercise. $\triangledown$

Theorem 22.9. Let $F \subseteq K$ be an extension and $f \in F[x]$. Then $a \in K$ is a multiple zero of f if and only if a is a zero of both f and f'. Hence, f has a multiple zero in its splitting field if and only if $\gcd(f, f') \neq 1$.

Proof. In class. $\triangledown$

Example. Consider $f = 2x^5 + x^3 - x \in \mathbb{Z}_3[x]$, where $f' = x^4 - 1$ and $\gcd(f, f') = x^2 + 1$. (Verify!) Since $\gcd(f, f') \neq 1$, we see that f and f' have a common zero in some extension field. In fact, f factors over $\mathbb{Z}_3$ as $2x^5 + x^3 - x = 2x(x^2 + 1)^2$, hence the roots $\pm i \in \mathbb{Z}_3(i)$ each has multiplicity two.

Exercise 22. Complete this homework set before we continue to the next section.

1) Let a have minimal polynomial f over F. Prove that if n is the least integer for which there exist $c_0, \dots, c_{n-1} \in F$ such that $a^n = \sum_{k=0}^{n-1} c_k a^k$, then $f = x^n - \sum_{k=0}^{n-1} c_k x^k$.
2) Find the minimal polynomial over $\mathbb{Q}$ for $a =$ (a) $\sqrt{1 + 3\sqrt{2}} \in \mathbb{R}$ (b) $\sqrt{7} - \sqrt{5} \in \mathbb{R}$ (c) $i\sqrt{i} \in \mathbb{C}$ (d) $i + 2\sqrt{i} \in \mathbb{C}$.
3) Determine if $f \in F[x]$ has a multiple zero in its splitting field: (a) $x^3 - 3x - 2 \in \mathbb{Q}[x]$ (b) $3x^{20} - x^5 + 2x + 1 \in \mathbb{Z}_5[x]$ (c) $x^5 - 2x^3 + 2x \in \mathbb{Z}_5[x]$ (d) $2x^7 + 3x^5 - 1 \in \mathbb{Z}_7[x]$.
4) Prove that $\mathbb{Q}(i + \sqrt{2}) \approx \mathbb{Q}(\sqrt{1 - 2i\sqrt{2}})$ using Corollary 22.4.

23 Finite Fields

Definition. By a *finite field* we mean a field with only finitely many elements, e.g., $\mathbb{Z}_7$.

Lemma 23.1. Let G be a finite group with identity e. Suppose that $x^k = e$ has at most k roots in G for each $k \geq 1$. Then G is cyclic.

Proof. Let $|G| = n$. For each $a \in G$ the cyclic subgroup $\langle a \rangle$ has order $d \mid n$. And each $x \in \langle a \rangle$ is a root of $x^d = e$, hence *all* the roots to $x^d = e$ are given by $\langle a \rangle$. In particular if an element $g \in G$ has order d then $g \in \langle a \rangle$ and $\langle g \rangle = \langle a \rangle$. So *if* there is an element of order d in G then there are exactly $\phi(d)$ elements of order d. But recall (see Theorem 7.6 and its remark) that $n = \sum \phi(d)$, where d ranges through all the divisors of n. It follows that G *does* have $\phi(d)$ elements of order d for each $d \mid n$. In particular there is an element of order n, hence G is cyclic. ▽

Theorem 23.2. Let F be a finite field. The multiplicative group F^* is cyclic.

Proof. This follows from the lemma because the group is finite and the polynomial $x^k - 1$ has at most k zeros over any field. ▽

Corollary 23.3. If p is a prime, the group U_p is cyclic.

Proof. U_p is the multiplicative group of nonzero elements of the finite field $\mathbb{Z}_p$. ▽

Definition. The *characteristic* of a field F, denoted by $\chi(F)$, is the additive order of 1, the unity of F. However, if $|1| = \infty$, we let $\chi(F) = 0$, e.g., $\chi(\mathbb{Z}_p) = p$ and $\chi(\mathbb{Q}) = 0$.

Theorem 23.4. If $\chi(F) \neq 0$, then $\chi(F)$ is prime. In particular, the characteristic of a finite field is always a prime number.

Proof. Let $\chi(F) = n > 1$. We write $n \cdot 1$ instead of $\sum_1^n 1$. Now if $n = ab$ with $a, b < n$, then $0 = n \cdot 1 = ab \cdot 1 = a \cdot 1 \times b \cdot 1$. Either $a \cdot 1 = 0$ or $b \cdot 1 = 0$ since a field has no zero divisors, contradicting the minimality of n. Hence $\chi(F)$ must be a prime number. ▽

Lemma 23.5. If $\chi(F) = p$, a prime, then F is an extension field over $\mathbb{Z}_p$. If $\chi(F) = 0$, then F is an extension over $\mathbb{Q}$.

Proof. Define $\theta : \mathbb{Z} \to F$ by $\theta(n) = n \cdot 1$. It is easy to verify that this map is a ring homomorphism. If $\chi(F) = 0$ then θ is one-to-one, in which case F contains $\mathbb{Z}$, as well as $\mathbb{Q}$ since F is a field. If $\chi(F) = p$ then $\ker(\theta) = (p)$ and F contains $\mathbb{Z}/(p) \approx \mathbb{Z}_p$. ▽

Theorem 23.6. The number of elements in any finite field F is a prime power p^k, for some integer k and prime number $p = \chi(F)$.

Proof. By the lemma, F is an extension over $\mathbb{Z}_p$, where $p = \chi(F)$. Since F is finite, it has a finite basis over $\mathbb{Z}_p$ as a vector space, say $\{a_1, \ldots, a_k\}$. (This is a linear algebra fact which will be discussed again in Section 25.) Every element in F is then uniquely determined by the form $\sum c_i a_i$, where $0 \leq c_i \leq p - 1$. Thus $|F| = p^k$. ▽

Lemma 23.7. If $\chi(F) = p$ then $(a + b)^p = a^p + b^p$ for all $a, b \in F$.

Proof. According to the binomial theorem,

$$(a+b)^p = \sum_{k=0}^{p} \left(\begin{array}{c} p \\ k \end{array} \right) a^{p-k} b^k \quad \text{where} \quad \left(\begin{array}{c} p \\ k \end{array} \right) = \frac{p\,!}{k\,!\,(p-k)\,!}$$

The prime p divides all the binomial coefficients, except for $k = 0$ and $k = p$, where they equal 1. Since $\chi(F) = p$, multiples of p vanish. Hence $(a+b)^p = a^p + b^p$. ▽

Theorem 23.8. Let $q = p^k$, a prime power. There exists a field F with q elements.

Proof. We consider an extension K over $\mathbb{Z}_p$ where $x^q - x = (x - a_1) \cdots (x - a_q) \in K[x]$ based on Corollary 22.6. Note that elements of $\mathbb{Z}_p$ are among the zeros. We claim that $F = \{a_1, \ldots, a_q\}$ is a subfield of K by showing that it is closed under addition and multiplication. For all $a, b \in F$ we have $(ab)^q = a^q b^q = ab$ and, by the lemma and induction on k, $(a+b)^q = ((a+b)^p)^{p^{k-1}} = (a^p + b^p)^{p^{k-1}} = a^q + b^q$. To complete the proof, we make sure that there is no multiple zero. This follows from Theorem 22.9 because $(x^q - x)' = qx^{q-1} - 1 = -1$ as $\chi(K) = p$. ▽

Remark. The equality $x^q - x = (x - a_1) \cdots (x - a_q)$ holds in $F[x]$, for any finite field F with q elements (Exercise 20.4). The proof above then implies that $F = \mathbb{Z}_p(a_1, \ldots, a_q)$, the splitting field of $x^q - x$ over $\mathbb{Z}_p$. Later, in Theorem 28.1, we will prove that splitting fields are unique for a given polynomial, but for now we show that finite fields are unique for a fixed q.

Theorem 23.9. Any two finite fields of order $q = p^k$ are isomorphic.

Proof. Call the fields K and L, both extensions over $\mathbb{Z}_p$. By Theorem 23.2 we assume $K^* = \langle a \rangle$, so that $K = \mathbb{Z}_p(a) \approx \mathbb{Z}_p[x]/(f)$, where f is the minimal polynomial of a over $\mathbb{Z}_p$. By Theorem 22.2, $f \mid x^q - x$ in $\mathbb{Z}_p[x]$. But $x^q - x = (x - b_1) \cdots (x - b_q) \in L[x]$, hence $f(b) = 0$ for some $b \in L$. Thus f is also the minimal polynomial of b over $\mathbb{Z}_p$ and, Corollary 22.4 implies $K \approx \mathbb{Z}_p(b)$, a subfield of L. We conclude that $K \approx L$ because they have equal size. ▽

Definition. Without ambiguity, we now denote a finite field of order $q = p^k$ using the notation $\mathbb{F}_q$. The multiplicative group $\mathbb{F}_q^*$, consisting of the $q - 1$ nonzero elements, is cyclic with $\phi(q-1)$ generators. In particular, $\mathbb{F}_p = \mathbb{Z}_p$ and $\mathbb{F}_p^* = U_p$.

Example. The polynomial $f = x^2 + x + 1$ is irreducible over $\mathbb{Z}_2$. (Why?) The field $\mathbb{Z}_2[x]/(f)$ has order 4 since it is represented by $a + bx$ with $a, b \in \{0, 1\}$. This is the field $\mathbb{F}_4 = \{0, 1, \alpha, 1+\alpha\}$, where α satisfies $\alpha^2 + \alpha + 1 = 0$, or $\alpha^2 = 1 + \alpha$. We construct the Cayley tables for $\mathbb{F}_4$ below. Note that α and $1+\alpha$ are the two generators for $\mathbb{F}_4^*$.

$+$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

$\times$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

Example. Similarly, $f = x^2 - 2$ is irreducible over $F = \mathbb{Z}_{11}$ and the factor ring $F[x]/(f)$ is the finite field $\mathbb{F}_{121}$. In this case, $\mathbb{F}_{121}^*$ has $\phi(120) = 32$ generators. In general, the field $\mathbb{Z}_p[x]/(f)$ has p^n elements, if $f \in \mathbb{Z}_p[x]$ is an irreducible polynomial of degree n.

Theorem 23.10. The finite field $\mathbb{F}_{p^k}$ has a subfield $\mathbb{F}_q$ if and only if $q = p^j$ with $j \mid k$.

Proof. Having the same characteristic, a subfield of $\mathbb{F}_{p^k}$ is clearly $\mathbb{F}_{p^j}$ with $j \leq k$. Looking at the multiplicative groups, we have $p^j - 1 \mid p^k - 1$, which holds if and only if $j \mid k$. (Why?) Conversely, let $j \mid k$. Then $x^{p^j-1} - 1 \mid x^{p^k-1} - 1$ and so the zeros of $x^{p^j} - x$, which compose $\mathbb{F}_{p^j}$, are zeros of $x^{p^k} - x$, which form $\mathbb{F}_{p^k}$. Thus $\mathbb{F}_{p^j} \subseteq \mathbb{F}_{p^k}$. $\bigtriangledown$

Example. The above theorem allows us to identify all the subfields of a given finite field $\mathbb{F}_q$ in much a similar way we do for groups using a subgroup lattice. The following diagram depicts the *subfield lattice* for $\mathbb{F}_{3^{12}}$.

$$\begin{tikzcd}
 & & \mathbb{F}_{3^{12}} \arrow[dl, no head] \arrow[dr, no head] & \\
 & \mathbb{F}_{3^6} \arrow[dl, no head] \arrow[dr, no head] & & \mathbb{F}_{3^4} \arrow[dl, no head] \\
\mathbb{F}_{3^3} \arrow[dr, no head] & & \mathbb{F}_{3^2} \arrow[dl, no head] & \\
 & \mathbb{F}_3 & &
\end{tikzcd}$$

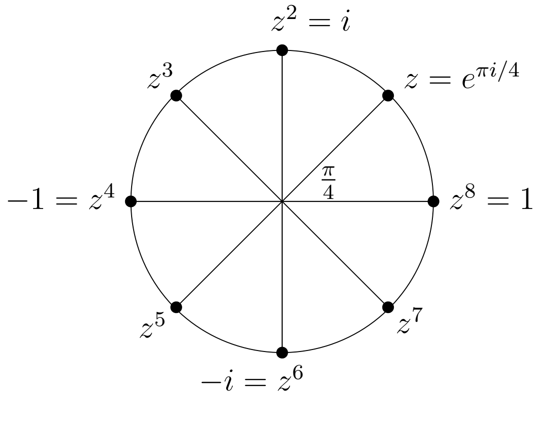
Exercise 23. Complete this homework set before we continue to the next section.

1) Let F be a finite field with $\chi(F) = p$. Prove that $F = \{a^p \mid a \in F\}$ by establishing the isomorphism $\theta : F \to F$ defined by $\theta(a) = a^p$ for all $a \in F$.
2) Construct the Cayley tables (both $+$ and $\times$) for the finite field (a) $\mathbb{Z}_2[x]/(x^3+x+1)$ (b) $\mathbb{Z}_3[x]/(x^2+1)$.
3) Show how to construct the finite field $\mathbb{F}_q$ for $q =$ (a) 16 (b) 25 (c) 27 (d) 32.
4) Let F be a field of 2048 elements. Prove that $F = \mathbb{Z}_2(a)$, for any element $a \in F^*$ other than the unity.

24 Cyclotomic Polynomials

Definition. By an nth *root of unity* we mean a zero of $x^n - 1$ in some splitting field over the underlying field in context. This root is *primitive* if it is not a zero of $x^k - 1$ for any $k < n$.

Example. The nth roots of unity in $\mathbb{C}$ are given by $z, z^2, \ldots, z^n = 1$, where $z = e^{2\pi i/n}$. The graph below roughly displays the coordinates of the eight complex eighth roots of unity, which are proportionally dispersed along the unit circle in the complex plane.



Theorem 24.1. Let $z = e^{2\pi i/n} \in \mathbb{C}$. There are exactly $\phi(n)$ primitive nth roots of unity, given by z^k for all positive integers k less than and relatively prime to n.

Proof. The multiplicative cyclic subgroup $\langle z\rangle$ has order n. The primitive nth roots of unity are precisely the generators of $\langle z\rangle$; and the proof is all group theory. $\triangledown$

Definition. Let $z_1, \dots, z_{\phi(n)}$ denote the $\phi(n)$ distinct primitive nth roots of unity in $\mathbb{C}$. The nth *cyclotomic polynomial* is given by $\Phi_n = (x - z_1)\cdots(x - z_{\phi(n)}) \in \mathbb{C}[x]$. Note that Φ_n is monic, of degree $\phi(n)$, and has no multiple zeros. In fact all the $\phi(n)$ zeros of Φ_n in $\mathbb{C}$ are the $\phi(n)$ distinct primitive nth roots of unity.

Example. We have $\Phi_1 = x - 1$ and $\Phi_2 = x + 1$, whereas Φ_3 can be computed as follows.

$$\Phi_3 = (x - e^{2\pi i/3})(x - e^{4\pi i/3}) = \left(x - \frac{-1 + i\sqrt{3}}{2}\right)\left(x - \frac{-1 - i\sqrt{3}}{2}\right) = x^2 + x + 1$$

Theorem 24.2. The factorization $x^n - 1 = \prod_{d|n} \Phi_d$ holds over $\mathbb{C}$.

Proof. Consider $G = \langle z\rangle$ again, partition it into subsets $G_d = \{a \in G \mid |a| = d\}$. Note that G_d is nonempty if and only if $d \mid n$. Now $a \in G_d$ if and only if a is a primitive dth root of unity. Hence, $x^n - 1 = \prod_{a\in G}(x - a) = \prod_{d|n}\prod_{a\in G_d}(x - a) = \prod_{d|n}\Phi_d$. $\triangledown$

Example. The above theorem can be used to compute Φ_n for all $n > 1$ in a recursive manner. For example, $x^4 - 1 = \Phi_1\Phi_2\Phi_4 = (x - 1)(x + 1)\Phi_4$, from which we are able to derive Φ_4—and similarly for other values of n—by performing long division, e.g.,

$$\begin{aligned}
\Phi_4 &= x^2 + 1 & \Phi_{12} &= x^4 - x^2 + 1\\
\Phi_6 &= x^2 - x + 1 & \Phi_{14} &= x^6 - x^5 + x^4 - x^3 + x^2 - x + 1\\
\Phi_8 &= x^4 + 1 & \Phi_{15} &= x^8 - x^7 + x^5 - x^4 + x^3 - x + 1\\
\Phi_9 &= x^6 + x^3 + 1 & \Phi_{16} &= x^8 + 1\\
\Phi_{10} &= x^4 - x^3 + x^2 - x + 1 & \Phi_{18} &= x^6 - x^3 + 1
\end{aligned}$$

Missing from the above list, when n is prime, Φ_n is given by the next theorem.

Theorem 24.3. If p is a prime then $\Phi_p = 1 + x + x^2 + \cdots + x^{p-1}$.

Proof. Since $x^p - 1 = \Phi_1\Phi_p$ then we have $\Phi_p = (x^p - 1)/(x - 1)$. $\triangledown$

You might think that the coefficients of Φ_n are only ±1. That is false, but you will not see a counter-example until Φ_{105}. What is true, though, they are integers always:

Theorem 24.4. The cyclotomic polynomials Φ_n belong to $\mathbb{Z}[x]$ for all $n \geq 1$.

Proof. We use induction based on $x^n - 1 = \prod_{d|n}\Phi_d$, which allows us to assume $x^n - 1 = f\Phi_n$ for some monic polynomial $f \in \mathbb{Z}[x]$. This shows that $\Phi_n \in \mathbb{Q}[x]$ by the division algorithm there. Then by Gauss' lemma, $\Phi_n \in \mathbb{Z}[x]$ since it is monic. $\triangledown$

Definition. We name the extension $\mathbb{Q}(z)$ the nth *cyclotomic field* over $\mathbb{Q}$ if z is a primitive nth root of unity in $\mathbb{C}$. Note that $\mathbb{Q}(z) = \mathbb{Q}(z^k)$ if and only if $\gcd(k, n) = 1$, hence the notation $\mathbb{Q}(z)$ is not dependent on which primitive root we choose.

Theorem 24.5. The nth cyclotomic field $\mathbb{Q}(z)$ is isomorphic to $\mathbb{Q}[x]/(\Phi_n)$.

Proof. This follows from the next theorem, which asserts that Φ_n is irreducible, thus establishing it as the minimal polynomial of z over $\mathbb{Q}$. $\triangledown$

Theorem 24.6. The cyclotomic polynomial Φ_n is irreducible over $\mathbb{Q}$.

Proof. Assume that $\Phi_n = fg \in \mathbb{Z}[x]$, both monic and f is chosen irreducible. Let z be a primitive nth root of unity for which $f(z) = 0$, hence f is the minimal polynomial of z over $\mathbb{Q}$. Choose a prime p as long as $p \nmid n$, so that z^p is another primitive root. Then z^p is a zero of either f or g. We will first show that $g(z^p) = 0$ is impossible.

If $g(z^p) = 0$ then z is a zero of $g(x^p)$ and $f \mid g(x^p)$. We may write $fh = g(x^p) \in \mathbb{Z}[x]$. Reducing mod p, we have $f'h' = g'(x^p) \in \mathbb{Z}_p[x]$, degrees unchanged. But by Lemma 23.7 $g'(x^p) = g'(x)^p$ in $\mathbb{Z}_p[x]$, where unique factorization applies. Here any irreducible factor of f' divides g' as well. Thus $f'g' = \Phi_n'$ implies that Φ_n' has multiple zeros, hence $x^n - 1$ does as well, over $\mathbb{Z}_p$. This is banned by Theorem 22.9: the derivative is $nx^{n-1} \neq 0$; only 0 is zero, and 0 is never a root of unity.

So we have $f(z^p) = 0$. Now a typical primitive nth root of unity is z^k with $\gcd(k, n) = 1$. In that case $k = p_1 \cdots p_r$, not assumed distinct, such that $p_i \nmid n$. Writing $z^k = (z^{p_1})^{p_2 \cdots p_r}$ we see by induction that $f(z^k) = 0$—for all $\phi(n)$ values of k. This can happen only if $f = \Phi_n$, irreducible over $\mathbb{Z}$, and over $\mathbb{Q}$ by Gauss' lemma. $\triangledown$

Exercise 24. Complete this homework set before we continue to the next section.

1) Compute Φ_n for each value of $n \leq 30$.
2) Verify the following identities.
   a) $\Phi_n(0) = 1$ for all $n \geq 2$
   b) $\Phi_{2^n}(x) = x^{2^{n-1}} + 1$ for all $n \geq 1$
   c) $\Phi_{2n}(x) = \Phi_n(-x)$ for all odd $n \geq 3$
   d) $\Phi_{n^2}(x) = \Phi_n(x^n)$ for all $n \geq 1$
3) Where p is prime, prove that Φ_p is irreducible over $\mathbb{Q}$ using Eisenstein's criterion and the substitution $x = t + 1$.
4) Prove that $\gcd(x^m - 1, x^n - 1) = x^{\gcd(m,n)} - 1$ in $\mathbb{Q}[x]$ by factoring both of them into cyclotomic polynomials.

25 Algebraic Extensions

Definition. Let K be an extension field over F. The *degree* $[K{:}F]$ of K over F is the dimension of K as a vector space over F. If this degree is a finite number, we say that the field K is a *finite extension* over F, otherwise *infinite*.

Theorem 25.1. Let $F \subseteq L \subseteq K$ be a tower of fields. Then $[K{:}F] = [K{:}L] \times [L{:}F]$ if finite, and in particular, $[L{:}F] \mid [K{:}F]$. Hence, a finite extension over another finite extension is finite over the bottom field.

Proof. The proof can be found in a linear algebra text. $\triangledown$

Definition. The *degree* of $a \in K$ over F is the degree of the minimal polynomial of a over F. If $a \in K$ is not algebraic over F, then a is called a *transcendental* element. Hence, we may say that a transcendental element of K over F has an infinite degree.

It is known, for instance, that the real numbers π and e are both transcendental over $\mathbb{Q}$; but this fact is not easy to demonstrate.

Theorem 25.2. The element $a \in K$ is algebraic of degree n over F if and only if $[F(a){:}F] = n$. Hence a is transcendental if and only if $F(a)$ is an infinite extension over F.

Proof. We have seen that $F[x]/(f) = \{(f) + a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} \mid a_i \in F\}$, where $n = \deg f$. In this case $\{1, x, \ldots, x^{n-1}\}$ is a basis of $F[x]/(f)$ over F. Hence if a is algebraic, then $\{1, a, \ldots, a^{n-1}\}$ is a basis of $F(a)$ over F and $[F(a){:}F] = n$. Conversely if $[F(a){:}F] = n$, then the set $\{1, a, \ldots, a^n\}$ is linearly dependent, i.e., there exists $g \in F[x]$ such that $g(a) = 0$ and so a is algebraic. By Theorem 22.3, $[F[x]/(f){:}F] = n$, where f is the minimal polynomial of a over F. Hence $\deg f = n$. $\triangledown$

Example. The nth cyclotomic field $\mathbb{Q}(z)$ is an extension of degree $\phi(n)$ over $\mathbb{Q}$, because the minimal polynomial of z is given by Φ_n, whose degree is $\phi(n)$. On the other hand, the extension $\mathbb{R}$ over $\mathbb{Q}$ is infinite. To see it, simply consider the intermediate subfield $\mathbb{Q}(\pi)$, trusting that π is transcendental.

Lemma 25.3. If $a, b \neq 0$ are algebraic over F then $a \pm b, ab, ab^{-1}$ are algebraic over F.

Proof. We have field extensions $F \subseteq F(a) \subseteq (F(a))(b) = F(a, b)$, where each is finite over the one below it, according to Theorem 25.2. By Theorem 25.1 $F(a, b)$ is finite over F and, being a field, it contains $a \pm b, ab, ab^{-1}$. Hence by Theorem 25.2 again, all these elements are also algebraic over F. $\triangledown$

Theorem 25.4. Let K be an extension field over F. The set of all elements in K which are algebraic over F is a subfield of K containing F.

Proof. This follows directly from the lemma. $\triangledown$

Theorem 25.5. Let K be the field of all real numbers which are algebraic over $\mathbb{Q}$. Then the degree $[K{:}\mathbb{Q}]$ is infinite.

Proof. The polynomial $x^n - 2$ is irreducible according to Eisenstein's criterion. Hence the real number $\sqrt[n]{2}$ is algebraic of degree n over $\mathbb{Q}$. It follows that $[\mathbb{Q}(\sqrt[n]{2}){:}\mathbb{Q}] = n$ and $[K{:}\mathbb{Q}] \geq n$. Since n is arbitrary, K must be an infinite extension. $\triangledown$

Definition. The extension field K over F is called an *algebraic extension* if every element $a \in K$ is algebraic over F.

Theorem 25.6. The extension field K over F is finite if and only if K is an algebraic extension over F in the form $K = F(a_1, \ldots, a_n)$ for some elements $a_1, \ldots, a_n \in K$.

Proof. If $[K{:}F]$ is finite then so is $[F(a){:}F]$ for any $a \in K$ by Theorem 25.1, hence by Theorem 25.2, K is an algebraic extension. The elements $a_1, \ldots, a_n$ can be chosen from any basis of K over F as a vector space. Conversely, suppose $K = F(a_1, \ldots, a_n)$ is algebraic over F. Since $F \subseteq F(a_1) \subseteq (F(a_1))(a_2) \subseteq \cdots \subseteq K$ and each step is finite, then $[K{:}F]$ is finite by Theorem 25.1. $\triangledown$

Theorem 25.7. Algebraic extension over an algebraic extension is again algebraic, i.e., if L is algebraic over F and K is algebraic over L, then K is algebraic over F.

Proof. Let $a \in K$. Since a is algebraic over L, we have $b_0 + b_1 a + \cdots + b_n a^n = 0$ for some elements $b_i \in L$. These b_i's are algebraic over F, hence by Theorem 25.6, $[M{:}F]$ is finite where $M = F(b_0, \ldots, b_n)$. Also a is algebraic over M, hence by Theorem 25.2 $[M(a){:}M]$ is finite. By Theorem 25.1 then $M(a)$ is finite over F. But $M(a) = F(a, b_0, \ldots, b_n)$, hence by Theorem 25.6 again, a is algebraic over F. $\triangledown$

Exercise 25. Complete this homework set before we continue to the next section.

1) Find the degree of $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ over $\mathbb{Q}$ and find a basis for it.
2) Given that π is transcendental over $\mathbb{Q}$, show that $\pi^{2/3}$ is also transcendental.
3) Suppose that a and b are algebraic over F of degrees m and n, respectively. If $\gcd(m, n) = 1$, prove that $[F(a, b){:}F] = mn$.
4) The extension field K over F is called *simple* if $K = F(a)$ for some $a \in K$.

   a) Prove that any extension field of prime degree is simple.
   b) Prove that any finite extension over a finite field is simple.
   c) If $\chi(F) = 0$, it is known that $F(a, b)$ is simple for all algebraic elements $a, b \in K$. Use this fact to prove that any finite extension over $\mathbb{Q}$ is simple.
   d) Illustrate (c) by showing that $\mathbb{Q}(\sqrt{2}, \sqrt{5}) = \mathbb{Q}(\sqrt{2} + \sqrt{5})$.

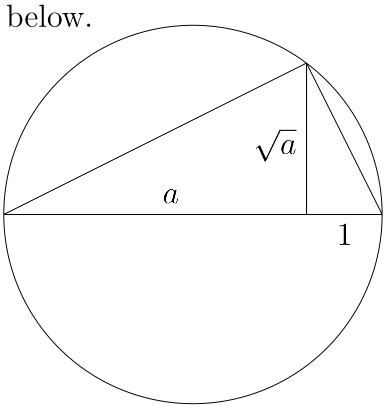
26 Applications in Classical Geometry

Consider the xy-plane of the usual cartesian coordinate system. A point on the plane is *constructible* if it can be traced out using only an unmarked ruler and a compass. The unit length is assumed, so that at least we are able construct all points with integer coordinates. By dropping perpendicular lines against the x and y-axes, we see that a point (a, b) is constructible if and only if the real number lengths a and b are constructible.

Theorem 26.1. The real numbers which are constructible form a subfield of $\mathbb{R}$.

Proof. Let $a, b \in \mathbb{R}$ be constructible. It is intuitively clear how to get the lengths $a \pm b$ using a ruler and a compass. It is also known how to construct two similar right-angle triangles $ABC \sim A'B'C'$. To construct ab we let $AB = 1$, $BC = a$, and $A'B' = b$. Then by the properties of similar triangles, we have $B'C' = ab$. To make $B'C' = 1/a$, simply let $AB = a$, $BC = 1$, and $A'B' = 1$. ▽

Example. The theorem implies that all rational numbers are constructible. To see an irrational number example, recall in grade school geometry how to construct $\sqrt{a}$ from a given length a, pictured below.



Theorem 26.2. The number $a \in \mathbb{R}$ is constructible only if a is algebraic over $\mathbb{Q}$ of degree a power of 2.

Proof. Consider equations of lines and circles with coefficients in $F = \mathbb{Q}$. We omit details, but any two such graphs only intersect at constructible coordinates belonging to F or to some quadratic extension $F(\sqrt{a_0})$. Constructible numbers are all obtained in this way, perhaps successively replacing F by $F_1 = F(\sqrt{a_0})$, then F_1 by $F_2 = F_1(\sqrt{a_1})$, and on. In each step we have $[F_n{:}\mathbb{Q}] = 2^n$. ▽

Remark. The proof actually gives a stronger statement: a is constructible only if $a \in F_n$ in some tower of extension fields $\mathbb{Q} \subset F_1 \subset \cdots \subset F_n \subset \mathbb{R}$, such that $F_{i+1} = F_i(\sqrt{a_i})$, of degree 2 over F_i. In fact, this is a necessary and sufficient condition to be constructible since, as seen in the previous example, square root numbers are constructible.

Example. A classical geometry challenge posed by the Greeks was to construct a square whose area equals that of a given circle. This is the famous *squaring the circle* problem. To construct such a square requires the length $\sqrt{\pi}$, which is not algebraic. With the theorem, we know why this challenge is impossible to answer.

Corollary 26.3. An arbitrary angle cannot be trisected.

Proof. We show as a counter-example that $\alpha = 60^o$ cannot be trisected because the number $a = \cos 20^o$ is not constructible. We use the trigonometric identity $\cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha$ to see that $8a^3 - 6a - 1 = 0$. Now the polynomial $8x^3 - 6x - 1$ is irreducible over $\mathbb{Q}$ because it has no zero mod 5, for instance. Hence $[\mathbb{Q}(a){:}\mathbb{Q}] = 3$, not a power of 2. $\triangledown$

Corollary 26.4. The regular heptagon is not constructible.

Proof. Let $\alpha = 2\pi/7$. To construct the heptagon it is necessary that both $\sin\alpha$ and $\cos\alpha$ be constructible, say they belong to some extension K of degree 2^n over $\mathbb{Q}$. Then the primitive seventh root of unity $z = \cos\alpha + i\sin\alpha$ belongs to $K(i)$, of degree 2 over K. Hence $[K(i){:}\mathbb{Q}] = 2^{n+1}$. But note that $\mathbb{Q}(z)$ is an intermediate subfield of degree $\phi(7) = 6$. Since $6 \nmid 2^{n+1}$, this whole thing is impossible. $\triangledown$

Definition. The *Fermat numbers* are given by $F_n = 2^{2^n} + 1$ for integers $n \geq 0$. A *Fermat prime* is a Fermat number which is also a prime number.

The first five Fermat numbers are Fermat primes: 3, 5, 17, 257, 65537. However, it is not yet known if there is any more Fermat prime.

Lemma 26.5. Any prime of the form $2^m + 1$ is a Fermat prime.

Proof. Exercise. $\triangledown$

Theorem 26.6. The regular polygon with n vertices is constructible only if n is a product of some power of 2 and distinct Fermat primes.

Proof. Generalizing from the case $n = 7$, the previous proof shows it necessary that $\phi(n)$ be a power of 2. If $n = 2^k \prod p_i^{e_i}$ then $\phi(n) = 2^{k-1} \prod p_i^{e_i - 1}(p_i - 1)$. Hence $e_i = 1$ for each i, and p_i is a power of 2 plus one. By the lemma each p_i is a Fermat prime. $\triangledown$

Remark. The converse of the theorem is good as well. In particular Gauss, who first proved it, actually constructed a regular 17-gon in his teenage years. But for us to prove it, we will have to wait for Galois theory.

Exercise 26. Complete this homework set before we continue to the next section.

1) Another ancient Greek problem is called *doubling the cube.* Can we construct a cube double the volume of another constructible cube?
2) Which ones of these angles of degree (a) 8 (b) 9 (c) 15 (d) 40 are constructible?
3) Suppose that there are no more Fermat primes to be discovered. How many regular polygons with an odd number of vertices can be constructed?
4) Using ruler and compass only, show how to construct a regular pentagon.

27 Galois Groups

By an *automorphism* of a field F we mean an isomorphism $\theta : F \to F$. The following are a few examples of a field automorphism.

1) Let $\theta : \mathbb{C} \to \mathbb{C}$ be given by $\theta(a + bi) = a - bi$ for all $a, b \in \mathbb{R}$. In particular, note that $\theta(a) = a$ for all $a \in \mathbb{R}$. It is not difficult to show that θ is an automorphism of the complex number field, by verifying that it is one-to-one, onto, and that $\theta((a+bi)+(c+di)) = \theta(a+bi)+\theta(c+di)$ and $\theta((a+bi)(c+di)) = \theta(a+bi)\theta(c+di)$.

2) The map $\theta(a + b\sqrt{2}) = a - b\sqrt{2}$ is an automorphism of the field $\mathbb{Q}(\sqrt{2})$.

3) In any field, the identity map is clearly an automorphism. So is the inverse map of any automorphism again an automorphism of the same field.

Definition. Let F be a field. Let $\mathrm{Aut}(F)$ denote the set of all automorphisms of F. We shall see that $\mathrm{Aut}(F)$ is a group, called the *automorphism group* of F, under the usual composition of functions.

Theorem 27.1. Given a field F, the set $\mathrm{Aut}(F)$ is a group under composition.

Proof. The identity map, which we shall denote ι, serves as the identity element in $\mathrm{Aut}(F)$. The inverse of $\theta \in \mathrm{Aut}(F)$ is simply the inverse map. Other details of the proof are left as an exercise. $\triangledown$

Theorem 27.2. Let K be an extension field over F. Then the set $S = \{\theta \in \mathrm{Aut}(K) \mid \theta(a) = a \text{ for all } a \in F\}$ is a subgroup of $\mathrm{Aut}(K)$.

Proof. It is clear that the identity map belongs to S. Equally obvious, if $\theta \in S$ so is $\theta^{-1} \in S$. Finally, if both $\theta(a) = a$ and $\psi(a) = a$, then $\psi \circ \theta(a) = a$ to assure that S is closed under composition. $\triangledown$

Definition. Let K be an extension field over F. The subgroup of $\mathrm{Aut}(K)$ given in the preceding theorem is called the *Galois group* of K over F, and it is denoted by $\mathrm{Gal}(K/F) = \{\theta \in \mathrm{Aut}(K) \mid \theta(a) = a \text{ for all } a \in F\}$. Conversely, if H is a subgroup of $\mathrm{Aut}(K)$ then we call $K_H = \{a \in K \mid \theta(a) = a \text{ for all } \theta \in H\}$ the *fixed field* of H. This term will be justified in the next theorem where we will see that K_H is indeed a field, i.e., a subfield of K. In particular, if $H \subseteq \mathrm{Gal}(K/F)$ then $K_H \supseteq F$.

Theorem 27.3. Let H be any subgroup of $\mathrm{Aut}(K)$. Then the set $K_H = \{a \in K \mid \theta(a) = a \text{ for all } \theta \in H\}$ is a subfield of K. In particular when H is finite, we have $[K{:}K_H] = |H|$.

Proof. Recall that $\theta(0) = 0$ and $\theta(1) = 1$ for any isomorphism. (The first equality already holds in any homomorphism.) It follows that both $0, 1 \in K_H$. Now given $a, b \in K_H$, we have $\theta(a - b) = \theta(a) - \theta(b) = a - b$ if $\theta \in H$, as well as $\theta(ab^{-1}) = \theta(a)\theta^{-1}(b) = ab^{-1}$. All these suffice to claim that K_H is indeed a subfield of K.

The second statement is not at all trivial. But we prefer to have you search for the proof independently, requiring pretty much a knowledge in linear algebra. $\triangledown$

Example. Let $\theta \in \mathrm{Aut}(\mathbb{C})$ as in the earlier example, where $\theta(a + bi) = a - bi$. We consider $\mathbb{C}$ as a field extension over $\mathbb{R}$, and note that $\theta \in \mathrm{Gal}(\mathbb{C}/\mathbb{R})$. If ι denotes the identity map then $\langle\theta\rangle = \{\iota, \theta\}$ is a subgroup of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$. In this case, $\mathbb{C}_{\langle\theta\rangle} = \mathbb{R}$.

Proposition 27.4. Let K be an extension field over F. Suppose that $\theta \in \mathrm{Gal}(K/F)$ and $f \in F[x]$. Then $a \in K$ is a zero of f if and only if $\theta(a)$ is too. In particular, both a and $\theta(a)$ must have the same minimal polynomial over F.

Proof. The key is in showing that $f(\theta(x)) = \theta(f(x))$—exercise. $\bigtriangledown$

Corollary 27.5. The complex number $a + bi$ is a zero of a polynomial $f \in \mathbb{R}[x]$ if and only if $a - bi$ is also a zero of f.

Proof. This follows from the example of $\theta(a + bi) = a - bi$. $\bigtriangledown$

Corollary 27.6. Every polynomial $f \in \mathbb{R}[x]$ is irreducible over $\mathbb{R}$ if and only if $f = Ax^2 + Bx + C$ with either $A = 0$ or $B^2 - 4AC < 0$.

Proof. Only the converse is unclear. By the fundamental theorem of algebra, f has at least one complex zero, and by the previous corollary we may assume that $a \pm bi$ are two zeros. Then $(x - a + bi)(x - a - bi) = (x - a)^2 + b^2$ is a factor of f over $\mathbb{R}$, hence f is reducible if $\deg f \geq 3$. $\bigtriangledown$

Theorem 27.7. Let K be an extension field over $\mathbb{Q}$. Then $\mathrm{Aut}(K) = \mathrm{Gal}(K/\mathbb{Q})$.

Proof. It suffices to show that if $\theta \in \mathrm{Aut}(K)$ then $\theta(a) = a$ for all $a \in \mathbb{Q}$. This holds since $\theta(1) = 1$ and for any $n \in \mathbb{Z}$ we have $\theta(n) = \theta(n \cdot 1) = n \cdot \theta(1) = n$ if $n \geq 0$. Similarly, if $n < 0$ we have $\theta(-n) = -n$, hence $\theta(n) = -\theta(-n) = n$. Lastly, if $m, n \in \mathbb{Z}$, $n \neq 0$, then $\theta(m/n) = \theta(mn^{-1}) = \theta(m)\theta(n)^{-1} = mn^{-1} = m/n$. $\bigtriangledown$

Example. Consider $\theta \in \mathrm{Aut}(\mathbb{Q}(\sqrt{2}))$. By our theorems, $\theta(a+b\sqrt{2}) = a+b\theta(\sqrt{2})$, where $\theta(\sqrt{2}) = \pm\sqrt{2}$, being the roots of $x^2 = 2$. Hence either $\theta = \iota$, the identity map, or else $\theta(a+b\sqrt{2}) = a-b\sqrt{2}$, in which case $\theta^2 = \iota$. Thus $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})) = \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \mathbb{Z}_2$.

Exercise 27. Complete this homework set before we continue to the next section.

1) Prove that if we have subgroups $H \subseteq H' \subseteq \mathrm{Aut}(K)$, then $K_H \supseteq K_{H'}$.
2) Prove that if we have subfields $L \subseteq L' \subseteq K$, then $\mathrm{Gal}(K/L) \supseteq \mathrm{Gal}(K/L')$.
3) Show that $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) \approx \mathbb{Z}_2 \times \mathbb{Z}_2$.
4) Show that $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q})$ has order 8.

28 Normal Extensions

Recall that a splitting field of a polynomial $f \in F[x]$ over F is $K = F(a_1, \ldots, a_n)$, where $a_1, \ldots, a_n$ are all the zeros of f in K. For example, the splitting field of $x^2 + 1$ over $\mathbb{Q}$ is $\mathbb{Q}(i)$. Note that over $\mathbb{R}$, the splitting field of $x^2 + 1$ would be $\mathbb{R}(i) = \mathbb{R}$, hence this definition is dependent upon the underlying field F. Nevertheless, the next theorem affirms that the splitting field of f over F is unique, up to isomorphism.

Theorem 28.1. Suppose that K and K' are both splitting fields of $f \in F[x]$ over F. Then $K \approx K'$, with an isomorphism θ such that $\theta(a) = a$ for all $a \in F$.

Proof. Let $[K : F] = n$. If $n = 1$ then f splits in F and $K = K' = F$ with nothing to prove. We proceed by induction. For $n > 1$, f has an irreducible factor g whose zeros are not in F. Let $a \in K$ and $b \in K'$ be zeros of g. Then $F(a) \approx F(b)$ by Corollary 22.4. Moreover both K and K' are splitting fileds of f/g over F, hence $K \approx K'$ by the induction hypothesis. $\bigtriangledown$

Definition. The *Galois group* of a polynomial $f \in F[x]$ refers to the Galois group $\mathrm{Gal}(K/F)$ where K is the (unique) splitting field of f over F.

Example. We have seen that the Galois group of $x^2 - 2$ over $\mathbb{Q}$ is $\{\iota, \theta\} \approx \mathbb{Z}_2$, where $\theta(a + b\sqrt{2}) = a - b\sqrt{2}$.

Theorem 28.2. Let $a, b \in K$, the splitting field of $f \in F[x]$. Then there exists $\theta \in \mathrm{Gal}(K/F)$ with $\theta(a) = b$ if and only if a and b have the same minimal polynomial over F.

Proof. Let a and b have the same minimal polynomial over F. Then $F(a) \approx F(b)$ by Corollary 22.4, with an isomorphism such that $\theta(a) = b$. This isomorphism can be extended over K as in the proof of the preceding theorem—exercise. The converse follows immediately by Proposition 27.4. $\triangledown$

Example. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, the splitting field of $(x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x]$. We see that every $\theta \in \mathrm{Gal}(K/\mathbb{Q})$ will be determined by the evaluations $\theta(\sqrt{2})$ and $\theta(\sqrt{3})$. Let us define $\theta(\sqrt{2}) = \sqrt{2}$ and $\theta(\sqrt{3}) = -\sqrt{3}$, together with $\psi(\sqrt{2}) = -\sqrt{2}$ and $\psi(\sqrt{3}) = \sqrt{3}$. Note that $\psi \circ \theta(\sqrt{2}) = -\sqrt{2}$ and $\psi \circ \theta(\sqrt{3}) = -\sqrt{3}$. The theorem affirms that $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \{\iota, \theta, \psi, \psi \circ \theta\}$. Looking at the order of each element here, it is not hard to deduce that this Galois group is none other than $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Definition. Let K be an algebraic extension field over F. We call K *normal* if for every irreducible polynomial $f \in F[x]$ with at least one zero in K, we have f splits over K, i.e., all its zeros in K.

For example, the field $\mathbb{C}$ is normal over $\mathbb{R}$ if you recall the fundamental theorem of algebra. On the other hand, the extension $\mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$ is not normal because it obviously contains one zero of $x^3 - 2 \in \mathbb{Q}[x]$ but not the other two complex zeros.

Normal extensions have to do with normal subgroups of their corresponding Galois groups. This is explained in the coming theorem, following the next lemma.

Lemma 28.3. Let K be a finite extension over F. Then K is normal if and only if K is the splitting field of some polynomial over F.

Proof. Being finite extension, $K = F(a_1, \ldots, a_n)$. Assume K is normal and let f_i be the minimal polynomial of a_i over F, which therefore splits in K. It follows that K is the splitting field of $\prod f_i \in F[x]$.

Conversely, suppose that K is the splitting field of $f \in F[x]$. Let $g \in F[x]$ be irreducible with one zero $a \in K$. To complete the proof, given another zero b of g, we will show that $b \in K$. Firstly, since g is irreducible, $F(a) \approx F(b)$ by Corollary 22.4. Secondly, we may say that $K(a)$ is the splitting field of f over $F(a)$ and, similarly, $K(b)$ of f over $F(b)$. In essence, by identifying $F(a)$ with $F(b)$, we see that $K(a) \approx K(b)$ with an isomorphism that leaves F fixed. However, $K(a) = K$, so we conclude that $[K(b){:}F] = [K{:}F]$, i.e., that $b \in K$. $\triangledown$

Theorem 28.4. Consider the finite tower $F \subseteq L \subseteq K$, where both extensions K and L are normal over F. Then $\mathrm{Gal}(K/L)$ is a normal subgroup of $\mathrm{Gal}(K/F)$, with the corresponding factor group $\mathrm{Gal}(K/F)/\mathrm{Gal}(K/L) \approx \mathrm{Gal}(L/F)$.

Proof. By the fundamental theorem of homomorphism, it suffices to construct a homomorphism $\Theta : \mathrm{Gal}(K/F) \to \mathrm{Gal}(L/F)$ which is onto and with $\ker(\Theta) = \mathrm{Gal}(K/L)$.

For every $\theta \in \mathrm{Gal}(K/F)$ we define $\theta' : L \to F$ by $\theta'(a) = \theta(a)$. We prove first that $\theta' \in \mathrm{Gal}(L/F)$—only one thing is unclear: that $\theta'(L) = L$. The lemma allows us to write $L = F(a_1, \dots, a_n)$, where a_i's are all the zeros of some $f \in F[x]$. Since then $\theta(a_i) = a_j$, we see that $F \subseteq \theta'(L) \subseteq L$ as subfields. At the same time, $\theta'(L) = \theta(L) \approx L$. Comparing degrees of extension forces $\theta'(L) = L$.

Hence we now define $\Theta(\theta) = \theta'$ and leave it an exercise to show that Θ is a homomorphism. Note that $\theta \in \ker(\Theta)$ if and only if $\theta \in \mathrm{Gal}(K/F)$ such that $\theta(a) = a$ for all $a \in L$, i.e., if and only if $\theta \in \mathrm{Gal}(K/L)$.

Finally to show onto, let $\theta' \in \mathrm{Gal}(L/F)$. We may consider K a splitting field over F, hence over L. The automorphism $\theta' : L \to L$ can therefore be extended to that of K, say $\theta \in \mathrm{Aut}(K)$, such that $\theta(a) = \theta'(a)$ for all $a \in L$ and in particular, $\theta(a) = a$ for all $a \in F$. Hence $\theta \in \mathrm{Gal}(K/F)$ and $\Theta(\theta) = \theta'$ as desired. $\bigtriangledown$

Exercise 28. Complete this homework set before we continue to the next section.

1) Show that the Galois group of $x^2 - 3$ over $\mathbb{Q}$ is the same as that of $x^2 - 2x - 2$.
2) Describe the Galois group of $x^3 - 5$ over $\mathbb{Q}$.
3) In the finite tower $F \subseteq L \subseteq K$, explain why if K is normal over F, then K is also normal over L.
4) An algebraic extension K is *separable* over F when the minimal polynomial of every $a \in K$ has distinct zeros in its splitting field. In the algebraic tower $F \subseteq L \subseteq K$, show that if K is separable over F, so are K over L and L over F.

29 The Galois Correspondence

The main results of Galois theory will now be presented, but only over fields of characteristic zero, e.g., $F = \mathbb{Q}$. They generalize over fields of prime characteristic, provided that the extension field in consideration is separable. (See the preceding exercise.) In particular, next exercise, it can be shown that any extension over a field of characteristic zero is separable.

Definition. Let K be a finite extension over F, where $\chi(F) = 0$. We call K a *Galois* extension when $|\mathrm{Gal}(K/F)| = [K{:}F]$.

Theorem 29.1. If $\chi(F) = 0$ and K is a Galois extension over F, then $K_{\mathrm{Gal}(K/F)} = F$.

Proof. Write $G = \mathrm{Gal}(K/F)$ so we have $|G| = [K{:}F]$ and $F \subseteq K_G \subseteq K$. But also $[K{:}K_G] = |G|$ by Theorem 27.3. Thus $[K_G{:}F] = 1$ and $K_G = F$. $\bigtriangledown$

Indeed we are almost ready to establish the fundamental theorem of Galois theory. However, given the purpose of this independent study, we will state the theorem without proof, while at this point you should be able to comprehend what need to be verified in order to claim the following statement.

Theorem 29.2 (Fundamental Theorem of Galois Theory)**.** Let K be a Galois extension over a field F with $\chi(F) = 0$. Then there is a one-to-one correspondence between the intermediate subfields L, where $F \subseteq L \subseteq K$, and the subgroups H of $\mathrm{Gal}(K/F)$. The subfield L corresponds to the subgroup $\mathrm{Gal}(K/L)$, where $K_{\mathrm{Gal}(K/L)} = L$; and the subgroup H corresponds to the subfield K_H, where $\mathrm{Gal}(K/K_H) = H$.

Example. Consider the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ discussed in the preceding section, whose Galois group $\{\iota, \theta, \psi, \psi \circ \theta\}$ is determined by $\theta(\sqrt{2}) = \sqrt{2}$, $\theta(\sqrt{3}) = -\sqrt{3}$, and $\psi(\sqrt{2}) = -\sqrt{2}$, $\psi(\sqrt{3}) = \sqrt{3}$. This is a Galois extension since both the degree of the extension and the order of the group equal four. We illustrate the fundamental theorem by producing the two lattices side-by-side, for the subgroups and the subfields.

$$\begin{tikzcd}
 & \{\iota, \theta, \psi, \psi \circ \theta\} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\{\iota, \theta\} \arrow[dr, dash] & \{\iota, \psi \circ \theta\} \arrow[d, dash] & \{\iota, \psi\} \arrow[dl, dash] \\
 & \{\iota\} &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & \mathbb{Q}(\sqrt{2}, \sqrt{3}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{6}) \arrow[d, dash] & \mathbb{Q}(\sqrt{3}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Over fields of characteristic zero, a Galois extension is not distinguished from a normal extension, which in turn is just the splitting field of some polynomial over the base field. This is stated as the next lemma, whose proof you are challenged to construct and which leads to a second main result of Galois theory.

Lemma 29.3. Let K be a finite extension over a field F of characteristic zero. Then K is Galois over F if and only if K is normal over F.

Theorem 29.4. Consider the tower $F \subseteq L \subseteq K$, where K is Galois over F and $\chi(F) = 0$. Then L is Galois over F if and only if $\mathrm{Gal}(K/L)$ is normal in $\mathrm{Gal}(K/F)$, in which case $\mathrm{Gal}(K/F)/\mathrm{Gal}(K/L) \approx \mathrm{Gal}(L/F)$.

Proof. Together with the lemma, necessity has been proved in Theorem 28.4. Your next project is to establish sufficiency—and to complete all the missing details of the other proofs in this section. $\bigtriangledown$

Exercise 29. Complete this homework set before we continue to the next section.

1) Let $\chi(F) = 0$ and $f \in F[x]$ be irreducible. Use Theorem 22.9 to show that f has no multiple zeros in its splitting field.
2) Let $\chi(F) = p$, a prime number, and $f \in F[x]$ be irreducible. Prove that f has multiple zeros if and only if $f \in F[x^p]$.
3) Verify the fundamental theorem of Galois theory by comparing the subgroup lattice for the Galois group and the subfield lattice for the splitting field of each $f \in \mathbb{Q}[x]$: (a) $x^2 - 5$ (b) $x^4 - 3$ (c) $x^4 - x^2 - 2$ (d) $x^4 + x^3 + x^2 + x + 1$.
4) Prove that the Galois group of $x^p - 1$ over $\mathbb{Q}$ is $\mathbb{U}_p$ if p is a prime. For $p = 17$, in particular, explain why there is a tower of subgroups of order 1, 2, 4, 8, 16, so that each extension in the corresponding subfield tower has degree two. This leads to the fact that the 17th root of unity is constructible, and so is the regular 17-gon. Use this observation to write the proof for the converse of Theorem 26.6.

30 Solvable Polynomials

As we know, the quadratic equation $ax^2 + bx + c = 0$ can be solved by an algorithm that involves only addition, multiplication, and the extraction of radicals, in this case $\sqrt{b^2 - 4ac}$. This claim remains valid, in particular, with the biquadratic equation

$ax^4 + bx^2 + c = 0$ upon the substitution $x^2 = t$. In the exercises, you will be guided to demonstrate that a general cubic equation can also be solved by radicals in this sense. This concept of solvability leads to the following definition.

Definition. A polynomial $f \in \mathbb{Q}[x]$ is *solvable* (by radicals) if there exists a tower of subfields $\mathbb{Q} \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_s \subseteq \mathbb{C}$, where K_s is the splitting field of f, such that for each $i < s$, the subfield $K_{i+1} = K_i(a_i)$ for some $a_i \in \mathbb{Z}$ and such that $a_i^{n_i} \in K_i$ for some $n_i \in \mathbb{Z}$.

Example. The polynomial $f(x) = x^4 - 2$ is clearly solvable by radicals. To meet the definition, we construct the tower $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})(i) = \mathbb{Q}(\sqrt[4]{2}, i)$, noting that the four zeros of f are $\pm\sqrt[4]{2}$ and $\pm i\sqrt[4]{2}$.

As a motivational application of Galois theory, some quintic polynomials will prove not solvable. It is not a coincidence that the next definition of a solvable group looks curiously familiar, in view of the Galois correspondence with the tower of subfields from a solvable polynomial.

Definition. A group G is *solvable* if there is a tower of subgroups $\{e\} \subseteq G_1 \subseteq G_2 \subseteq \cdots \subseteq G_s = G$ such that for each $i < s$, the subgroup G_i is normal in G_{i+1} and such that the factor group G_{i+1}/G_i is abelian.

For example, every abelian group G is readily solvable as we may let $s = 1$ in the above definition. Also, it follows from the definition of simple groups that a non-abelian simple group, e.g., the alternating group A_5, is never solvable.

The truth is, a polynomial $f \in \mathbb{Q}[x]$ is solvable if and only if its Galois group is. We will discuss only half of this remarkable fact, but enough to see why some polynomials are not solvable by radicals.

Lemma 30.1. Let F be a field of characteristic zero and $a \in F$. Then the Galois group of $x^n - a$ over F is solvable.

Proof. The splitting field of $x^n - a$ is $F(z, r)$, where z is any primitive nth root of unity and $r = \sqrt[n]{a} \in \mathbb{R}$. Consider first the case $z \in F$ and let $\theta, \psi \in \mathrm{Gal}(F(r)/F)$. These two elements are determined by their evaluation on r, being zeros of the same minimal polynomial, say $\theta(r) = rz^j$ and $\psi(r) = rz^k$ for some appropriate exponents j and k. Then

$$\psi \circ \theta(r) = \psi(r)\psi(z^j) = rz^k z^j = rz^j z^k = \theta(r)\theta(z^k) = \theta \circ \psi(r)$$

since both automorphisms leave z fixed. This shows that $\mathrm{Gal}(F(r)/F)$ is abelian, hence solvable. Now for the case $z \notin F$, we look at the tower $F \subseteq F(z) \subseteq F(z, r)$. Since $F(z)$ is the splitting field of $x^n - 1$ over F, Galois theory applies to give the corresponding subgroup tower

$$\{e\} \subseteq \mathrm{Gal}(F(z, r)/F(z)) \subseteq \mathrm{Gal}(F(z, r)/F)$$

As we have just demonstrated, $\mathrm{Gal}(F(z, r)/F(z))$ is abelian and we know that it is normal in $\mathrm{Gal}(F(z, r)/F)$ with factor group $\mathrm{Gal}(F(z)/F)$. It then suffices to show that $\mathrm{Gal}(F(z)/F)$ is abelian in order to conclude that $\mathrm{Gal}(F(z, r)/F)$ is solable. This is quite similar as before, for if $\theta, \psi \in \mathrm{Gal}(F(z)/F)$ then $\theta(z) = z^j$ and $\psi(z) = z^k$ (being nth roots of unity). It follows that $\psi \circ \theta(z) = \theta \circ \psi(z)$. And again such automorphisms are determined on z, so that $\psi \circ \theta = \theta \circ \psi$ as expected. ▽

Theorem 30.2. If $f \in \mathbb{Q}[x]$ is solvable, then the Galois group of f over $\mathbb{Q}$ is solvable.

Proof. Here is the sketch. The preceding lemma makes way to use a proof by induction. Along the way, you will need to verify the facts that given a group G with a normal subgroup H, then G/H is solvable if G is, and G is solvable if H and G/H are. $\bigtriangledown$

Example. Let $f = 2x^5 - 14x + 7$, which is irreducible over $\mathbb{Q}$ by Eisenstein's criterion. Using a graphing calculator one can check that f has exactly 3 real zeros, a, b, c; hence there is a conjugate pair z, z' of complex zeros to make the five of them. If G is the Galois group then every automorphism in G is determined by a permutation of these five zeros. Thus G can be viewed as a subgroup of the symmetric group S_5.

Since $[\mathbb{Q}(a){:}\mathbb{Q}] = 5$ we see that the splitting field of f is an extension of degree a multiple of 5 over $\mathbb{Q}$. So is $|G|$ a multiple of 5 according to Galois theory and in turn, by Cauchy's theorem, there must be an element of order 5 in G, say $(1, 2, 3, 4, 5) \in G$. Moreover, there is the 2-cycle corresponding to the permutation that swaps z and z', say $(1, 2) \in G$. Now it is not hard to show that $(1, 2, 3, 4, 5)$ and $(1, 2)$ generate all of S_5, i.e., that $G = S_5$. And finally, yet another exercise, you can verify that S_5 is not solvable, confirming that f is not solvable by radicals.

Exercise 30. Complete this homework set before we continue to the next section.

1) Solve the cubic equation $ax^3 + bx^2 + cx + d = 0$ in the following manner.
   a) Substitute $x = y - b/(3a)$ to get $y^3 + py + q = 0$.
   b) Substitute $y = \sqrt[3]{z} - p/(3\sqrt[3]{z})$ to get $27z^2 + 27qz - p^3 = 0$.
   c) Solve for z and back substitute to find x.
   d) Illustrate using the example $x^3 + 4x^2 + 4x + 3 = 0$.
2) Show that the Galois group of $x^4 - 2$ over $\mathbb{Q}$ is the dihedral group D_4, then prove that D_n in general is a solvable group.
3) Prove that a subgroup of a solvable group is again solvable. Hence, A_n is another evidence that the symmetric group S_n is not solvable for all $n \geq 5$.
4) Verify that $\{(1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$ is a normal subgroup of S_4 and use this fact to prove that S_4 is solvable. Hence, every polynomial of degree four over $\mathbb{Q}$ is solvable by radicals.

Supplementary Reading List

As an undergraduate algebra textbook, Gallian is perhaps the most readable, whereas Herstein a more concentrated classic. The remaining titles that make the recommended list below are self-descriptive of the specific topics they each deal with, and they are intended for more advanced studies.

1. Joseph A. Gallian, *Contemporary Abstract Algebra,* 10th ed., CRC Press 2021.
2. I. N. Herstein, *Topics in Algebra,* 2nd ed., Wiley 1975.
3. John F. Humphreys, *A Course in Group Theory,* Oxford University Press 1996.
4. Daniel A. Marcus, *Number Fields,* Springer 1977, 2018.
5. Gary L. Mullen and Carl Mummert, *Finite Fields and Applications,* AMS 2007.
6. Pierre Samuel, *Algebraic Theory of Numbers,* Hermann 1970, Dover 2008.
7. Ian Stewart, *Galois Theory,* 4th ed., CRC Press 2015.