Introduction to Abstract Algebra (Math 113)

Alexander Paulin, with edits by David Corwin

FOR FALL 2019 MATH 113 002 ONLY

Contents

1 Introduction

1.1 What is Algebra?

If you ask someone on the street this question, the most likely response will be: "Something horrible to do with x, y and z". If you're lucky enough to bump into a mathematician then you might get something along the lines

of: "Algebra is the abstract encapsulation of our intuition for composition". By composition, we mean the concept of two object coming together to form a new one. For example adding two numbers, multiplying two numbers, or composing real valued single variable functions. As we shall discover, the seemly simple idea of composition hides vast hidden depth.

Algebra permeates all of our mathematical intuitions. In fact the first mathematical concepts we ever encounter are the foundation of the subject. Let me summarize the first six to seven years of your mathematical education:

The concept of *Unity*. The number 1.

You probably always understood this, even as a little baby.

$\downarrow$

$\mathbb{N} := \{1, 2, 3...\}$, the natural numbers. $\mathbb{N}$ comes equipped with two natural operations $+$ and $\times$.

$\downarrow$

$\mathbb{Z} := \{... - 2, -1, 0, 1, 2, ...\}$, the integers.

We form these by using geometric intuition thinking of $\mathbb{N}$ as sitting on a line. $\mathbb{Z}$ also comes with $+$ and $\times$. Addition on $\mathbb{Z}$ has particularly good properties, e.g. additive inverses exist.

$\downarrow$

$\mathbb{Q} := \{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\}$, the rational numbers. We form these by taking $\mathbb{Z}$ and *formally* dividing through by non-negative integers. We can again

use geometric insight to picture $\mathbb{Q}$ as points on a line. The rational numbers also come equipped with $+$ and $\times$. This time, multiplication is has particularly good properties, e.g non-zero elements have multiplicative inverses.

We could continue by going on to form $\mathbb{R}$, the real numbers and then $\mathbb{C}$, the complex numbers. The motivation for passing to $\mathbb{R}$ is about analysis rather than algebra (limits rather than binary operations). But $\mathbb{R}$ has binary operations of addition and multiplication just like $\mathbb{Q}$, so one may still study it in the context of algebra.

Notice that at each stage the operations of $+$ and $\times$ gain additional properties. These ideas are very simple, but also profound. We spend years understanding how $+$ and $\times$ behave in $\mathbb{Q}$. For example

$$a + b = b + a \text{ for all } a, b \in \mathbb{Q},$$

or

$$a \times (b + c) = a \times b + a \times c \text{ for all } a, b, c \in \mathbb{Q}.$$

The central idea behind abstract algebra is to define a larger class of objects (sets with extra structure), of which $\mathbb{Z}$ and $\mathbb{Q}$ are definitive members.

$$\begin{aligned} (\mathbb{Z}, +) &\longrightarrow \textit{Groups} \\ (\mathbb{Z}, +, \times) &\longrightarrow \textit{Rings} \\ (\mathbb{Q}, +, \times) &\longrightarrow \textit{Fields} \end{aligned}$$

In linear algebra the analogous idea is

$$(\mathbb{R}^n, +, \text{scalar multiplication}) \longrightarrow \textit{Vector Spaces over } \mathbb{R}$$

The amazing thing is that these vague ideas mean something very precise and have far far more depth than one could ever imagine.

1.2 Sets

A set is any collection of objects. For example six dogs, all the protons on Earth, every thought you've ever had, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Observe that $\mathbb{Z}$ and

$\mathbb{Q}$ are sets with extra structure coming from $+$ and $\times$. In this whole course, all we will study are sets with some carefully chosen extra structure.

Basic Logic and Set Notation

Writing mathematics is fundamentally no different than writing English. It is a language which has certain rules which must be followed to accurately express what we mean. Because mathematical arguments can be highly intricate it is necessary to use simplifying notation for frequently occurring concepts. I will try to keep these to a minimum, but it is crucial we all understand the following:

- If P and Q are two statements, then $P \Rightarrow Q$ means that if P is true then Q is true. For example: x odd $\Rightarrow x \neq 2$. We say that P implies Q.
- If $P \Rightarrow Q$ and $Q \Rightarrow P$ then we write $P \Leftrightarrow Q$, which should be read as P is true if and only if Q is true.
- The symbol $\forall$ should be read as "for all".
- The symbol $\exists$ should be read as "there exists". The symbol $\exists!$ should be read as "there exists unique".

Let S and T be two sets.

- If s is an object contained in S then we say that s is an *element*, or a *member* of S. In mathematical notation we write this as $s \in S$. For example $5 \in \mathbb{Z}$. Conversely $s \notin S$ means that x is not contained in S. For example $\frac{1}{2} \notin \mathbb{Z}$.
- If S has finitely many elements then we say it is a finite set. We denote its cardinality (or size) by $|S|$.

- The standard way of writing down a set S is using *curly bracket* notation.

  $S = \{$ Notation for elements in S $\mid$ Properties which specifies being in S $\}$.

  The vertical bar should be read as "such that". For example, if S is the set of all even integer then

  $$S = \{x \in \mathbb{Z} \mid 2 \text{ divides } x\}.$$

  We can also use the curly bracket notation for finite sets without using the | symbol. For example, the set S which contains only 1,2 and 3 can be written as

  $$S = \{1, 2, 3\}.$$

- If every object in S is also an object in T, then we say that S is contained in T. In mathematical notation we write this as $S \subset T$, and in English we say that S *is a subset of* T. Note that $S \subset T$ and $T \subset S$ $\Rightarrow S = T$. If S is *not* contained in T we write $S \not\subset T$.

- If $S \subset T$ then $T \backslash S := \{x \in T \mid x \notin S\}$. $T \backslash S$ is called the *complement* of S in T.

- The set of objects contained in both S and T is call the intersection of S and T. In mathematical notation we denote this by $S \cap T$.

- The collection of all objects which are in either S or T is call the union on S and T. In mathematical notation we denote this by $S \cup T$.

- $S \times T = \{(a, b) \mid a \in S, b \in T\}$. We call this new set the (Cartesian) product of S and T. We may naturally extend this concept to finite collections of sets.

- The set which contains no objects is called the empty set. We denote the empty set by $\emptyset$. We say that S and T are *disjoint* if $S \cap T = \emptyset$. The union of two disjoint sets is often written as $S \coprod T$.

- A set is *finite* if it has finitely many elements. A more formal definition is that S is finite if there is an integer $n \in \mathbb{Z}_{\geq 0}$ such that there is a bijection from S to the set $\{1, 2, \cdots, n\}$ (note that this is the empty set if $n = 0$).

We recommend looking at `https://math.berkeley.edu/~gbergman/ug.hndts/sets_etc,t=1.pdf` for a guide to basic logic and set notation. We also **highly recommend** Section 6 of that article for some subtleties about the use of English in the logic of mathematical proofs.

1.3 Functions

Definition 1.1. A map (or function) f from S to T is a *rule* which assigns to each element of S a unique elements of T. We express this information using the following notation:

$$\begin{array}{rcl} f : S & \to & T \\ x & \mapsto & f(x) \end{array}$$

Here are some examples of maps of sets:

1. $S = T = \mathbb{N}$,

$$\begin{array}{rcl} f : \mathbb{N} & \to & \mathbb{N} \\ a & \mapsto & a^2 \end{array}$$

2. $S = \mathbb{Z} \times \mathbb{Z}$, $T = \mathbb{Z}$,

$$\begin{array}{rcl} f : \mathbb{Z} \times \mathbb{Z} & \to & \mathbb{Z} \\ (a, b) & \mapsto & a + b \end{array}$$

This very simple looking abstract concept hides enormous depth. To illustrate this, observe that calculus is just the study of certain classes of functions (continuous, differentiable or integrable) from $\mathbb{R}$ to $\mathbb{R}$.

Definition 1.2. Let S and T be two sets, and let $f : S \to T$ be a map.

1. We say that S is the *domain* (also known as *source*) of f and T is the *codomain* (also known as *target*) of f.

2. We say that f is the *identity* map if $S = T$ and $f(x) = x$, $\forall x \in S$. In this case we write $f = Id_S$.

Observe that if R, S, and T are sets, and $f\colon R \to S$ and $g\colon S \to T$ are maps, then we may compose them to give a new function: $g \circ f\colon R \to T$. Note that this is only possible if the domain of g is the same as the codomain of f.

Remark 1.3. We say that composition of functions is *associative*. This means that if R, S, T, and U are sets, and $f\colon R \to S$, $g\colon S \to T$, and $h\colon T \to U$ are maps, then the functions

$$(h \circ g) \circ f\colon R \to U$$

and

$$h \circ (g \circ f)\colon R \to U$$

are the same function.

You might be surprised to see the word "codomain" where you might be used to seeing the word "range". In fact, we will also talk about the range (or "image"), of a function, but it is not the same thing as codomain:

Definition 1.4. Let S and T be two sets, and let $f : S \to T$ be a map. We define the *image* (also known as *range*) of f to be:

$$\mathrm{Im}(f) := \{y \in T \mid \exists x \in S \text{ such that } f(x) = y\}$$

For example, if $S = T = \mathbb{R}$, and f is the function sending x to x^2, then the *codomain* of f is $\mathbb{R}$, but the *image* (or range) of f is only $\mathbb{R}_{\geq 0} = \{x \in \mathbb{R} \mid x \geq 0\}$.

Definition 1.5. Let $f\colon S \to T$, and suppose $U \subseteq T$. Then we define the *preimage* of U under f to be

$$f^{-1}(U) \coloneqq \{s \in S \mid f(s) \in U\}$$

.

Note that $f^{-1}(T) = S$ always. In fact, $f^{-1}(Im(f)) = S$. In general, $f^{-1}(U)$ is a subset of S.

1. f is *injective* if $f(x) = f(y) \Rightarrow x = y \; \forall \; x, y \in S$.
2. f is *surjective* if given $y \in T$, there exists $x \in S$ such that $f(x) = y$.
3. If f is both injective and surjective we say it is *bijective*. Intuitively this means f gives a perfect matching of elements in S and T.
4. If there is a bijection between S and T then we that S and T are *in bijection*.

Remark 1.6. The codomain and image of f are the same if and only if f is surjective.

Remark 1.7. If S and T are finite, then they are in bijection if and only if they have the same number of elements. More general, for infinite sets, one defines what it means to "have the same number of elements" by saying that two sets have the same number of elements if they are in bijection.

Remark 1.8. A set is infinite if and only if it has the same number of elements as a proper subset of itself. (In particular, if S is finite, then any proper subset of S has strictly fewer elements than S.)

Exercise 1.1. Let S and T be two sets. Let f be a map from S to T. Show that f is a bijection if and only if there exists a map g from T to S such that $f \circ g = Id_T$ and $g \circ f = Id_S$.

Definition 1.9. Let f be a map from S to T.

1. A *left inverse* for f is a map $g \colon T \to S$ such that $g \circ f = Id_S$.
2. A *right inverse* for f is a map $g \colon T \to S$ such that $f \circ g = Id_T$.

For example, let $S = \{1, 2, 3\}$ and $T = \{1, 2, 3, 4, 5\}$, and let $f(x) = x$ for $x \in S$. Define $g \colon T \to S$ so that $g(x) = x$ for $1 \leq x \leq 3$, and $g(4) = g(5) = 1$. Then g is a left inverse for f but **not** a right inverse. One can show that f does not have a right inverse because it is not surjective.

In this language, Exercise 1.1 is asking you to show that f is a bijection if and only if there is a map g that is both a left **and** right inverse for f.

Algebra is the general study of *laws of composition* or *binary operations*. The notion of function just defined allows us to formally define the notion of a *binary operation* on a set.

Definition 1.10. Let S be a set. Then a *binary operation* $*$ on S is a function

$$*\colon S \times S \to S.$$

We often write $a * b$ in place of $*(a, b)$, for $a, b \in S$.

Example 1.11.

1. Let S be either $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, or $M_n(\mathbb{R})$. Then both $+$ and $\times$ define binary operations.
2. If S is $\mathbb{R}$ or $\mathbb{Z}$, then the function $x * y = x^2 + 2y + 1$ defines a binary operation on S. Note that this is not associative like the previous examples.
3. Here's a nonexample. If $S = \{-1, 0, 1, 2, 3, \cdots\}$ is the set of integers greater than or equal to -1, then addition does NOT define a binary operation on S. That's because the codomain of a binary operation is always the original set S, but $-1 + (-1)$ is NOT in S.

Note that some books define the notion of a binary operation that is "closed" and will say that the last example is not closed. But for us, we will simply say that that last example is not a binary operation in the first place.

1.4 Equivalence Relations

Within a set it is sometimes natural to talk about different elements being related in some way. For example, in $\mathbb{Z}$ we could say that $x, y \in \mathbb{Z}$ are related if $x - y$ is divisible by 2. Said another way, x and y are related is they are both odd or both even. This idea can be formalized as something called an *equivalence relation*.

Definition 1.12. A *relation* on a set S is a subset $U \subset S \times S$. (This is also sometimes called a homogeneous relation, such as at `https://en.wikipedia.org/wiki/Binary_relation#Definition`.)

We often denote the relation by $\sim$. In this case, we write $x \sim y$ if and only if $(x, y) \in U$.

Definition 1.13. An equivalence relation on a set S is a subset $U \subset S \times S$ satisfying:

1. $(x, y) \in U \Leftrightarrow (y, x) \in U$. (This is called the symmetric property.)
2. $\forall x \in S, (x, x) \in U$. (This is called the reflexive property.)
3. Given $x, y, z \in S$, $(x, y) \in U$ and $(y, z) \in U \Rightarrow (x, z) \in U$. (This is called the transitive property.)

If $U \subset S \times S$ is an equivalence relation then we say that $x, y \in S$ are *equivalent* if and only if $(x, y) \in U$. In more convenient notation, we write $x \sim y$ to mean that x and y are equivalent.

Definition 1.14. Let $\sim$ be an equivalence relation on the set S. Let $x \in S$. The equivalence class containing x is the subset

$$[x] := \{y \in S \mid y \sim x\} \subset S.$$

Remark 1.15.
1. Notice that the reflexive property implies that $x \in [x]$. Hence equivalence classes are non-empty and their union is S.
2. The symmetric and transitive properties imply that $y \in [x]$ if and only if $[y] = [x]$. Hence two equivalence classes are equal or disjoint. It should also be noted that we can represent a given equivalence class using any of its members using the $[x]$ notation.

Definition 1.16. Let S be a set. Let $\{X_i\}$ be a collection of subsets for $i \in I$, some index set. We say that $\{X_i\}$ forms a partition of S if each X_i is non-empty, they are pairwise disjoint and their union is S.

We've seen that the equivalence classes of an equivalence relation naturally form a partition of the set. Actually there is a converse: Any partition of a set naturally gives rise to an equivalence relation whose equivalence classes are the members of the partition. The conclusion of all this is that an equivalence relation on a set is the same as a partition. In the example given above, the equivalence classes are the odd integers and the even integers. **Equivalence relations and equivalence classes are incredibly important. They will the foundation of many concepts throughout the course. Take time to really internalize these ideas.**

If $f\colon S \to I$ is a surjective map, then $S_i \coloneqq f^{-1}(\{i\})$ for $i \in I$ forms a partition of S. Conversely, any partition of S (indexed by a set I) leads to a surjective map from S to I.

So in fact, the following three concepts are essentially the same:

1. Equivalence relations on S
2. Partitions of S
3. Surjective maps with domain S

Specifically, an equivalence relation leads to a partition by equivalence classes, and conversely a partition leads to an equivalence relation by saying that $x \sim y$ iff x and y are in the same S_i. A partition gives rise to a surjective map from S to the index set (so $s \in S$ maps to the unique $i \in I$ such that $s \in S_i$), and a surjective map $f\colon S \to I$ gives rise to a partition $S_i = f^{-1}(\{i\})$ as mentioned above.

In the case of the partition of $\mathbb{Z}$ into the even and odd numbers, these three are

1. We say $x \sim y$ iff x and y have the same parity (or equivalently, if $x - y$ is divisible by 2)
2. We partition $\mathbb{Z}$ into the set S_1 of odd numbers and the set S_2 of even numbers

3. We have a map $f\colon \mathbb{Z} \to \{0,1\}$ sending even numbers to 0 and odd numbers to 1

Note that two surjective maps $f\colon S \to I$ and $f'\colon S \to I'$ define the same equivalence relation (or equivalently, the same partition) if there is a bijection between I and I' that identifies f with f'. For example, whether our index set for even and odd is $\{0,1\}$ or $\{\text{even}, \text{odd}\}$, we get the same partition and same equivalence relation, even though we technically have different surjections (because their codomains are different). **So when we say that these three concepts are "essentially" the same, keep in mind that two different surjections can technically give rise to the same partition/equivalence relation. But any two such surjections are related in a certain way.**

2 The Structure of $+$ and $\times$ on $\mathbb{Z}$

2.1 Basic Observations

We may naturally express $+$ and $\times$ in the following set theoretic way:

$$\begin{aligned} +\,:\mathbb{Z}\times\mathbb{Z} &\to \mathbb{Z} \\ (a,b) &\mapsto a+b \end{aligned}$$

$$\begin{aligned} \times\,:\mathbb{Z}\times\mathbb{Z} &\to \mathbb{Z} \\ (a,b) &\mapsto a\times b \end{aligned}$$

Here are 4 elementary properties that $+$ satisfies:

- (Associativity): $a+(b+c)=(a+b)+c\ \forall a,b,c\in\mathbb{Z}$
- (Existence of additive identity) $a+0=0+a=a\ \forall a\in\mathbb{Z}$.
- (Existence of additive inverses) $a+(-a)=(-a)+a=0\ \forall a\in\mathbb{Z}$

- (Commutativity) $a + b = b + a \ \forall a, b \in \mathbb{Z}$.

Here are 3 elementary properties that $\times$ satisfy:

- (Associativity): $a \times (b \times c) = (a \times b) \times c \ \forall a, b, c \in \mathbb{Z}$
- (Existence of multiplicative identity) $a \times 1 = 1 \times a = a \ \forall a \in \mathbb{Z}$.
- (Commutativity) $a \times b = b \times a \ \forall a, b \in \mathbb{Z}$.

The operations of $+$ and $\times$ interact by the following law:

- (Distributivity) $a \times (b + c) = (a \times b) + (a \times c) \ \forall a, b, c \in \mathbb{Z}$.

From now on we'll simplify the notation for multiplication to $a \times b = ab$.

Remarks

1. Each of these properties is totally obvious but will form the foundations of future definitions: groups and rings.
2. All of the above hold for $+$ and $\times$ on $\mathbb{Q}$. In this case there is an extra property that non-zero elements have multiplicative inverses:

   $$\text{Given } a \in \mathbb{Q}\backslash\{0\}, \ \exists\, b \in \mathbb{Q} \text{ such that } ab = ba = 1.$$

   This extra property will motivate the definition of a field.
3. The significance of the Associativity laws is that summing and multiplying a finite collection of integers makes sense, i.e. is independent of how we do it.

It is an important property of $\mathbb{Z}$ (and $\mathbb{Q}$) that the product of two non-zero elements is again non-zero. More precisiely: $a, b \in \mathbb{Z}$ such that $ab = 0 \Rightarrow$

either $a = 0$ or $b = 0$. Later this property will mean that $\mathbb{Z}$ is something called an *integral domain*. This has the following useful consequence:

Cancellation Law: For $a, b, c \in \mathbb{Z}$, $ca = cb$ and $c \neq 0 \Rightarrow a = b$.

This is proven using the distributive law together with the fact that $\mathbb{Z}$ is an integral domain. I leave it an exercise to the reader.

You might wonder why we are making such a big point about the cancellation law - after all, you already know this from your previous experience with. The reason we emphasize it is that the cancellation law does not always hold in $\mathbb{Z}/m\mathbb{Z}$; it holds only for certain m.

2.2 Factorization and the Fundamental Theorem of Arithmetic

Definition 2.1. Let $a, b \in \mathbb{Z}$. Then a divides $b \Leftrightarrow \exists c \in \mathbb{Z}$ such that $b = ca$. We denote this by $a \mid b$ and say that a is a divisor (or factor) of b.

Observe that 0 is divisible by every integer. The only integers which divide 1 are 1 and -1. Any way of expressing an integer as the product of a finite collection of integers is called a *factorization*.

Definition 2.2. A prime number p is an integer greater than 1 whose only positive divisors are p and 1. A positive integer which is not prime is called *composite*.

Remark 2.3. $\mathbb{Z}$ is *generated* by 1 under addition. By this I mean that every integer can be attained by successively adding 1 (or -1) to itself. Under multiplication the situation is much more complicated. There is clearly no single generator of $\mathbb{Z}$ under multiplication in the above sense.

Definition 2.4. Let $a, b \in \mathbb{Z}$. The highest common factor of a and b, denoted $HCF(a, b)$, is the largest positive integer which is a common factor of a and b. It is also called $gcd(a, b)$. Two non-zero integers $a, b \in \mathbb{Z}$ are said to be *coprime* if $HCF(a, b) = 1$.

Here are some important elementary properties of divisibility dating back to Euclid (300BC), which I'll state without proof. We'll actually prove them later in far more generality.

Theorem 2.5 (Remainder Theorem)**.** *Given $a, b \in \mathbb{Z}$, if $b > 0$ then $\exists!\ q, r \in \mathbb{Z}$ such that $a = bq + r$ with $0 \leq r < b$.*

Theorem 2.6. *Given $a, b \in \mathbb{Z}$, $\exists u, v \in \mathbb{Z}$ such that $au + bv = HCF(a, b)$. In particular, a and b are coprime if an only if there exist $u, v \in \mathbb{Z}$ such that $au + bv = 1$.*

Euclid's Lemma. Let p be a prime number and $a, b \in \mathbb{Z}$. Then

$$p \mid ab \Rightarrow p \mid a \text{ or } p \mid b$$

Proof. If $p \nmid a$, then a and p are coprime. Therefore, we can find $u, v \in \mathbb{Z}$ such that $au + pv = 1$. But then $b = b(au + pv) = p(vb) + ab(u)$. Since $p \mid ab$, it must also divide $ab(u)$ and therefore $p(vb) + ab(u)$, so $p \mid b$. □

The Fundamental Theorem of Arithmetic. Every positive integer, a, greater than 1 can be written as a product of primes:

$$a = p_1 p_2 ... p_r.$$

Such a factorization is unique up to ordering.

Proof. If there is a positive integer not expressible as a product of primes, let $c \in \mathbb{N}$ be the least such element. The integer c is not 1 or a prime, hence $c = c_1 c_2$ where $c_1, c_c \in \mathbb{N}$, $c_1 < c$ and $c_2 < c$. By our choice of c we know that both c_1 and c_2 are the product of primes. Hence c much be expressible as the product of primes. This is a contradiction. Hence all positive integers can be written as the product of primes.

We must prove the uniqueness (up to ordering) of any such decomposition. Let

$$a = p_1 p_2 ... p_r = q_1 q_2 ... q_s$$

be two factorizations of a into a product of primes. Then $p_1 \mid q_1 q_2 ... q_s$. By Euclid's Lemma we know that $p_1 \mid q_i$ for some i. After renumbering we may

assume $i = 1$. However q_1 is a prime, so $p_1 = q_1$. Applying the cancellation law we obtain

$$p_2...p_r = q_2...q_s.$$

Assume that $r < s$. We can continue this process until we have:

$$1 = q_{r+1}..q_s.$$

This is a contradiction as 1 is not divisible by any prime. Hence $r = s$ and after renumbering $p_i = q_i \ \forall i$. □

Using this we can prove the following beautiful fact:

Theorem 2.7. *There are infinitely many distinct prime numbers.*

Proof. Suppose that there are finitely many distinct primes $p_1, p_2.....p_r$. Consider $c = p_1p_2...p_r + 1$. Clearly $c > 1$. By the Fundamental Theorem of Arithmetic, c is divisible by at least one prime, say p_1. Then $c = p_1d$ for some $d \in \mathbb{Z}$. Hence we have

$$p_1(d - p_2...p_r) = c - p_1p_2..p_r = 1.$$

This is a contradiction as no prime divides 1. Hence there are infinitely many distinct primes. □

The Fundamental Theorem of Arithmetic also tells us that every positive element $a \in \mathbb{Q}$ can be written uniquely (up to reordering) in the form:

$$a = p_1^{\alpha_1} \cdots p_n^{\alpha_n};\ p_i \text{ prime and } \alpha_i \in \mathbb{Z}$$

The Fundamental Theorem also tells us that two positive integers are coprime if and only if they have no common prime divisor. This immediately shows that every positive element $a \in \mathbb{Q}$ can be written uniquely in the form:

$$a = \frac{\alpha}{\beta}, \alpha, \beta \in \mathbb{N} \text{ and coprime.}$$

We have seen that both $\mathbb{Z}$ and $\mathbb{Q}$ are examples of sets with two concepts of composition ($+$ and $\times$) which satisfy a collection of abstract conditions. We have also seen that the structure of $\mathbb{Z}$ together with $\times$ is very rich. Can we think of other examples of sets with a concept of $+$ and $\times$ which satisfy the same elementary properties?

2.3 Congruences

Fix $m \in \mathbb{N}$. By the remainder theorem, if $a \in \mathbb{Z}, \exists\ !\ \ q, r \in \mathbb{Z}$ such that $a = qm + r$ and $0 \leq r < m$. We call r the *remainder* of a modulo m. This gives the natural equivalence relation on $\mathbb{Z}$:

$$a \sim b \Leftrightarrow a \text{ and } b \text{ have the same remainder modulo } m \Leftrightarrow m \mid (a - b)$$

Exercise 2.1. Check this really is an equivalence relation! (We did most of this in class.)

Definition. $a, b \in \mathbb{Z}$ are **congruent modulo m** $\Leftrightarrow m \mid (a - b)$. This can also be written:

$$a \equiv b \mod m.$$

Remark 2.8.

1. The equivalence classes of $\mathbb{Z}$ under this relation are indexed by the possible remainders modulo m. These possible remainders are the integers 0 through $m - 1$. Hence, there are m distinct equivalence classes which we call **residue classes**. We denote the set of all residue classes $\mathbb{Z}/m\mathbb{Z}$.

2. There is a natural surjective map

$$\begin{aligned} [\,] \ : \ & \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \\ & a \mapsto [a] \end{aligned} \tag{1}$$

   Note that this is clearly not injective as many integers have the same remainder modulo m. Also observe that $\mathbb{Z}/m\mathbb{Z} = \{[0], [1], ...[m-1]\}$.

The following result allows us to define + and × on $\mathbb{Z}/m\mathbb{Z}$.

Proposition. Let $m \in \mathbb{N}$. Then,$\forall a, b, a', b' \in \mathbb{Z}$:

$$[a] = [a'] \text{ and } [b] = [b'] \Rightarrow [a+b] = [a'+b'] \text{ and } [ab] = [a'b'].$$

Proof. This is a very good exercise. We went over it in class. □

Definition. We **define** addition and multiplication on $\mathbb{Z}/m\mathbb{Z}$ by

$$[a] \times [b] = [a \times b] \; \forall a, b \in \mathbb{Z} \qquad [a] + [b] = [a+b] \; \forall a, b \in \mathbb{Z}$$

Remark 2.9. Note that there is ambiguity in the definition, because it seems to depend on making a choice of representative of each residue class. The proposition shows us that the resulting residue classes are independent of this choice, hence + and × are well defined on $\mathbb{Z}/m\mathbb{Z}$. This means that addition and multiplication mod n are *well-defined*.

Our construction of + and × on $\mathbb{Z}/m\mathbb{Z}$ is lifted from $\mathbb{Z}$, hence they satisfy the eight elementary properites that + and × satisfied on $\mathbb{Z}$. In particular $[0] \in \mathbb{Z}/m\mathbb{Z}$ behaves like $0 \in \mathbb{Z}$:

$$[0] + [a] = [a] + [0] = [a], \; \forall [a] \in \mathbb{Z}/m\mathbb{Z};$$

and $[1] \in \mathbb{Z}/m\mathbb{Z}$ behaves like $1 \in \mathbb{Z}$:

$$[1] \times [a] = [a] \times [1] = [a], \; \forall [a] \in \mathbb{Z}/m\mathbb{Z}.$$

We say that $[a] \in \mathbb{Z}/m\mathbb{Z}$ is non-zero if $[a] \neq [0]$. Even though + and × on $\mathbb{Z}/m\mathbb{Z}$ share the same elementary properties with + and × on $\mathbb{Z}$, they behave quite differently in this case. As an example, notice that

$$[1] + [1] + [1] + \cdots + [1](m \text{ times}) = [m] = [0]$$

Hence we can add 1 (in $\mathbb{Z}/m\mathbb{Z}$) to itself and eventually get 0 (in $\mathbb{Z}/m\mathbb{Z}$).

Also observe that if m is composite with $m = rs$, where $r < m$ and $s < m$ then $[r]$ and $[s]$ are both non-zero ($\neq [0]$) in $\mathbb{Z}/m\mathbb{Z}$, but $[r] \times [s] = [rs] = [m] = [0] \in \mathbb{Z}/m\mathbb{Z}$. Hence we can have two non-zero elements *multiplying* together to give *zero*, unlike in $\mathbb{Z}$.

Proposition. For every $m \in \mathbb{N}, a \in \mathbb{Z}$ the congruence

$$ax \equiv 1 \mod m$$

has a solution (in $\mathbb{Z}$) iff a and m are coprime.

Proof. This is just a restatement of the fact that a and m coprime $\Leftrightarrow \exists u, v \in \mathbb{Z}$ such that $au + mv = 1$. □

Observe that the congruence above can be rewritten as $[a] \times [x] = [1]$ in $\mathbb{Z}/m\mathbb{Z}$. We say that $[a] \in \mathbb{Z}/m\mathbb{Z}$ has a multiplicative inverse if $\exists [x] \in \mathbb{Z}/m\mathbb{Z}$ such that $[a] \times [x] = [1]$. Hence we deduce that the only elements of $\mathbb{Z}/m\mathbb{Z}$ with muliplicative inverse are those given by $[a]$, where a is coprime to m.

Recall that $\mathbb{Q}$ had the extra property that all non-zero elements had *multiplicative inverses*. When does this happen in $\mathbb{Z}/m\mathbb{Z}$?. By the above we see that this can happen $\Leftrightarrow \{1, 2, \cdots, m-1\}$ are all coprime to m. This can only happen if m is prime. We have thus proven the following:

Corollary. All non-zero elements of $\mathbb{Z}/m\mathbb{Z}$ have a multiplicative inverse $\Leftrightarrow m$ is prime.

Later this will be restated as $\mathbb{Z}/m\mathbb{Z}$ is a *field* $\Leftrightarrow m$ is a prime. These are examples of things called *finite fields*.

Exercise 2.2. Show that if m is prime then the product of two non-zero elements of $\mathbb{Z}/m\mathbb{Z}$ is again non-zero.

Key Observation: There are naturally occuring sets (other than $\mathbb{Z}$ and $\mathbb{Q}$) which come equipped with a concept of $+$ and $\times$, whose most basic properties are the same as those of the usual addition and multiplication on $\mathbb{Z}$ or $\mathbb{Q}$. **Don't be fooled into thinking all other examples will come from numbers. As we'll see, there are many examples which are much more exotic**.

3 Groups

3.1 Basic Definitions

Definition. Let G be a set. A **binary operation** is a map of sets:

$$* : G \times G \to G.$$

For ease of notation we write $*(a, b) = a * b \; \forall a, b \in G$. Any binary operation on G gives a way of *combining* elements. As we have seen, if $G = \mathbb{Z}$ then $+$ and $\times$ are natural examples of binary operations. When we are talking about a set G, together with a fixed binary operation $*$, we often write $(G, *)$.

Fundamental Definition. A **group** is a set G, together with a binary operation $*$, such that the following hold:

1. (Associativity): $(a * b) * c = a * (b * c) \; \forall a, b, c \in G$.
2. (Existence of identity): $\exists e \in G$ such that $a * e = e * a = a \; \forall a \in G$.
3. (Existence of inverses): Given $a \in G, \exists b \in G$ such that $a * b = b * a = e$.

Remark 3.1. 1. We have seen five different examples thus far: $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Q}\backslash\{0\}, \times)$, $(\mathbb{Z}/m\mathbb{Z}, +)$, and $(\mathbb{Z}/m\mathbb{Z} \setminus \{[0]\}, \times)$ if m is prime. Another example is that of a real vector space under addition. Note that $(\mathbb{Z}, \times)$ is **not** a group. Also note that this gives examples of groups which are both finite and infinite. The more mathematics you learn the more you'll see that groups are *everywhere*.

2. A set with a single element admits one possible binary operation. This makes it a group. We call this the trivial group.

3. A set with a binary operation is called a **monoid** if only the first two properties hold. From this point of view, a group is a monoid in which every element is invertible. $(\mathbb{Z}, \times)$ is a monoid but not a group. We will not talk about monoids anymore, but it's good to know that the word exists.

4. Observe that in all of the examples given the binary operation is commutative, i.e. $a * b = b * a \ \forall a, b \in G$. We give this a name:

Definition. A group $(G, *)$ is called **Abelian** if it also satisfies

$$a * b = b * a \ \forall a, b \in G.$$

This is also called the commutative property.

The most basic Abelian group is $(\mathbb{Z}, +)$. Notice also that any vector space is an Abelian group under its natural addition.

You might be wondering why we care about groups that a not Abelian (or "non-abelian"). Here's an important example of a non-abelian group that you should have already seen in linear algebra:

$$\mathrm{GL}_n(\mathbb{R}) \coloneqq \{M \in M_n(\mathbb{R}) \mid \det(M) \neq 0\}.$$

Note that a square matrix has nonzero determinant if and only if it is invertible, i.e., has an inverse under matrix multiplication. This means that every element of $\mathrm{GL}_n(\mathbb{R})$ has an inverse under matrix multiplication. Because matrix multiplication is associative and because there is an identity matrix, $\{\mathrm{GL}_n(\mathbb{R}), \times\}$ forms a group. For $n \geq 2$, it is a *non-abelian* group.

Notice that elements of $\mathrm{GL}_n(\mathbb{R})$ can be thought of in a geometric way, as symmetries of $\mathbb{R}^n$, where the group operation is composition of symmetries (i.e., composition of linear transformations). We will eventually encounter many non-abelian groups related to symmetries of geometric objects.

So a group is a set with extra structure. In set theory we have the natural concept of a map between sets (a function). The following is the analogous concept for groups:

Fundamental Definition. Let $(G, *)$ and $(H, \circ)$ be two groups. A **homomorphism** f, from G to H, is a map of sets $f : G \to H$, such that $f(x * y) = f(x) \circ f(y)$ $\forall x, y \in G$. If $G = H$ and $f = Id_G$ we call f the identity homomorphism.

Remark 3.2.

1. Intuitively one should thing about a homomorphism as a map of sets which preserves the underlying group structure. It's the same idea as a linear map between vector spaces.
2. A homomorphism $f : G \to H$ which is bijective is called an **isomorphism**. Two groups are said to be **isomorphic** if there exists an isomorphism between them. Intuitively two groups being isomorphic means that they are the "same" group with relabelled elements.
3. A homomorphism from a group to itself (i.e. $f : G \to G$) is called an **endomorphism**. An endomorphism which is also an isomorphism is called an **automorphism**.

Example 3.3. Here are some examples of homomorphisms:

1. The inclusion map from $(\mathbb{Z}, +)$ into $(\mathbb{Q}, +)$ is a homomorphism. This is an example of an injective homomorphism that is not surjective.
2. The map from $(\mathbb{Z}, +)$ to $(\mathbb{Z}/m\mathbb{Z}, +)$ sending $a \in \mathbb{Z}$ to $[a] \in \mathbb{Z}/m\mathbb{Z}$ is a surjective homomorphism that is not injective.
3. For any group G, the identity map from G to itself is an automorphism of G.
4. Complex conjugation is an automorphism of $(\mathbb{C}, +)$.
5. The map from $\mathrm{GL}_n(\mathbb{R})$ to $(\mathbb{R} \setminus \{0\}, \times)$ sending a matrix A to its determinant $det(A)$ is a homomorphism. This is because $det(AB) = det(A)det(B)$.
6. The exponential function $x \mapsto e^x$ is a homomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R} \setminus \{0\}, \times)$. It is injective but not surjective.

7. The complex exponential $z \mapsto e^z$ from $(\mathbb{C}, +)$ to $(\mathbb{C} \setminus \{0\}, \times)$ is a homomorphism. In contrast with the real exponential function, it is surjective but not injective, because $e^z = e^{z+2\pi i}$.

8. The logarithm is a homomorphism from $(\mathbb{R}_{>0}, \times)$ to $(\mathbb{R}, +)$. In fact, it is an isomorphism.

9. For any group G and any group H, the map sending all elements of G to $e_H \in H$ is a homomorphism. It is the *trivial homomorphism* from G to H.

Proposition 3.4. *Let $(G, *), (H, \circ)$ and $(M, \square)$ be three groups. Let $f : G \to H$ and $g : H \to M$ be homomorphism. Then the composition $gf : G \to M$ is a homomorphism.*

Proof. Let $x, y \in G$. $gf(x * y) = g(f(x) \circ f(y)) = gf(x) \square gf(y)$. □

Remark 3.5. Composition of homomorphism gives the collection of endomorphisms of a group the structure of a monoid. The subset of automorphisms has the stucture of a group under composition. We denote it by $Aut(G)$. This is analogous to the collection of $n \times n$ invertible matrices being a group under matrix multiplication.

Proposition 3.6. *Let $(G, *)$ be a group. The identity element is unique.*

Proof. Assume $e, e' \in G$ both behave like the identity. Then $e = e * e' = e'$. □

Proposition 3.7. *Let $(G, *)$ be a group. For $a \in G$ there is only one element which behaves like the inverse of a.*

Proof. Assume $a \in G$ has two inverses, $b, c \in G$. Then:

$$\begin{aligned} (a * b) &= e \\ c * (a * b) &= c * e \\ (c * a) * b &= c \quad \text{(associativity and identity)} \\ e * b &= c \\ b &= c \end{aligned}$$

□

The first proposition tells us that we can write $e \in G$ for the identity and it is well-defined. Similarly the second proposition tells us that for $a \in G$ we can write $a^{-1} \in G$ for the inverse in a well-defined way. The proof of the second result gives a good example of how we prove results for abstract groups. We use only the axioms, nothing else.

Given $r \in \mathbb{Z}$ and $a \in G$, we write

$$a^r = \begin{cases} a * a * \cdots * a \ \ (r \text{ times}), & \text{if } r > 0 \\ e, & \text{if } r = 0 \\ a^{-1} * a^{-1} * \cdots * a^{-1} \ \ (-r \text{ times}), & \text{if } r < 0 \end{cases}$$

Cancellation Law for Groups. Let $a, b, c \in G$ a group. Then

$$a * c = a * b \Rightarrow c = b \text{ and } c * a = b * a \Rightarrow c = b$$

Proof. Compose on left or right by $a^{-1} \in G$, then apply the associativity and inverses and identity axioms. □

Remark 3.8. Here are a couple of facts that follow easily from the group axioms:

1. For any $x, y \in G$, where $(G, *)$ is a group, we have $(x*y)^{-1} = y^{-1}*x^{-1}$. To prove this, just check that $y^{-1} * x^{-1}$ is an inverse of $x * y$ using the associative property and the definition of x^{-1} and y^{-1}.
2. $(x * y)^{-1} = x^{-1} * y^{-1}$ iff $x * y = y * x$, i.e., iff x and y commute.
3. Similarly, $(x * y)^2 = x^2 * y^2$ iff $x * y = y * x$.

Proposition 3.9. *Let $(G, *)$ and $(H, \circ)$ be two groups and $f : G \to H$ a homomorphism. Let $e_G \in G$ and $e_H \in H$ be the respective identities. Then*

- $f(e_G) = e_H$.
- $f(x^{-1}) = (f(x))^{-1}, \forall x \in G$

Proof.

- $f(e_G) \circ e_H = f(e_G) = f(e_G * e_G) = f(e_G) \circ f(e_G)$. By the cancellation law we deduce that $f(e_G) = e_H$.
- Let $x \in G$. Then $e_H = f(e_G) = f(x * x^{-1}) = f(x) \circ f(x^{-1})$ and $e_H = f(e_G) = f(x^{-1} * x) = f(x^{-1}) \circ f(x)$. Hence $f(x^{-1}) = (f(x))^{-1}$.

□

3.1.1 Cayley Tables for Binary Operations and Groups

Recall that a binary operation on a set S is a map from $S \times S$ to S. We can express the set $S \times S$ as a grid or *table* whose rows and columns each respectively correspond to the elements of S. For finite S, we can actually draw this. For $S = \{a, b, c, d\}$, and we illustrate it as follows:

	a	b	c	d
a				
b				
c				
d				

Each empty cell in this table corresponds to a unique element of $S \times S$; for example, the pair (b, a) corresponds to the cell in the second row and first column (so the row always comes first in the pair). A binary operation on S is then simply a way of putting an element of S in each of the 16 cells of the table.

Example 3.10. Here's an example of a binary operation on S:

	a	b	c	d
a	a	b	c	d
b	a	c	a	d
c	d	b	d	c
d	b	c	a	a

This is what you know from grade school as a multiplication table. Many abstract algebra textbooks call it the *Cayley table* of the binary operation.

However, this binary operation does not make S into a group. To see why, we prove the following proposition:

Proposition 3.11. *In the Cayley table of a group G, every element of G appears exactly once in every row and in every column.*

Proof. To say that every row contains every element of G exactly once is to say that if $(G, *)$ is a group, then for fixed $a, b \in G$ the equation

$$a * x = b$$

has exactly one solution $x \in G$.

Similarly, to say that every column contains every element of G exactly once is to say that the equation

$$x * a = b$$

has exactly one solution.

Why is this true? Well, the fact that it has *at most* one solution is the Cancellation Law for groups, which we already proved.

How do we know that there is *at least one* solution? Well, for the row equation, we just take $x = a^{-1} * b$, and for the column equation, we take $x = b * a^{-1}$. □

How do we know that the Cayley table of Example 3.10 is not a group? We can note, for example, that the second row contains a twice rather than once (as well, we could note that it does not contain b).

As another example, we can consider $(\{0, 1\}, \times)$. The Cayley table is

	0	1
0	0	0
1	0	1

One can check that this is not a group because, for example, 0 appears twice in the first row.

Finally, let's give an example of the Cayley table of a binary operation that is actually a group. Specifically, here is the Cayley table of $(\mathbb{Z}/4\mathbb{Z}, +)$, where we let $a = [0]$, $b = [1]$, $c = [2]$, and $d = [3]$:

	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

Finally, here's another Cayley table of a group on the set $S = \{a, b, c, d\}$:

	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

This group is called the Klein Four-group[1]. Later, in Section 3.8, we will see that it is isomorphic to something we will call $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. It is also isomorphic to the group

$$\left(\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}, \times \right)$$

3.2 Subgroups, Cosets and Lagrange's Theorem

In linear algebra, we can talk about subspaces of vector spaces. We have an analogous concept in group theory.

[1]There is also a music group called the Klein Four Group, famous for `https://www.youtube.com/watch?v=BipvGD-LCjU`.

Intuitively, a subgroup H of $(G, *)$ is just a subset H of G that is a group under the *same operation* as G. Formally, we can define it as follows:

Definition. Let $(G, *)$ be a group. A **subgroup** of G is a subset $H \subset G$ such that

1. $e \in H$
2. $x, y \in H \Rightarrow x * y \in H$
3. $x \in H \Rightarrow x^{-1} \in H$

Remark 3.12. If H is a subgroup of G, and K is a subgroup of H (all with the same operation), then K is a subgroup of G.

Example 3.13.

1. If G is any group, then $\{e_G\}$ and G are both subgroups of G. The former is called the trivial subgroup. The latter is a non-proper subgroup (so all subgroups not equal to the whole group are called *proper subgroups*).
2. The group $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Q}, +)$, which is a subgroup of $(\mathbb{R}, +)$, which is itself a subgroup of $(\mathbb{C}, +)$.
3. The group $(\mathbb{Q}\backslash\{0\}, \times)$ is a subgroup of $(\mathbb{R}\backslash\{0\}, \times)$, which is a subgroup of $(\mathbb{C} \setminus \{0\}, \times)$.
4. The set of complex numbers with absolute value 1 is a subgroup of $(\mathbb{C} \setminus \{0\}, \times)$.
5. If $m \in \mathbb{Z}$, then the subset $m\mathbb{Z} := \{ma \mid a \in \mathbb{Z}\}$is a subgroup of $(\mathbb{Z}, +)$. Note that it is isomorphic to $(\mathbb{Z}, +)$.
6. If V is a vector space over $\mathbb{R}$ then it is naturally an Abelian group under addition. If W is a subspace then it is also under a subgroup under addition.
7. The set of purely imaginary numbers $\{ri \mid r \in \mathbb{R}\}$ is a subgroup of $(\mathbb{C}, +)$. Note that this is a special case of the previous example.
8. The set $\{\pm 1\}$ is a subgroup of $(\mathbb{Q} \setminus \{0\}, \times)$.
9. The set $\{2^n \mid n \in \mathbb{Z}\}$ of integer powers of 2 is a subgroup of $(\mathbb{Q}\backslash\{0\}, \times)$.

10. The set of matrices of the form

$$\left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{R}\, ac \neq 0 \right\}$$

is a subgroup of $\mathrm{GL}_2(\mathbb{R})$.

11. The subsets

$$\left\{ \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \mid a, c \in \mathbb{R}\, ac \neq 0 \right\}$$

and

$$\left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \mid b \in \mathbb{R} \right\}$$

are both subgroups of the group in the previous example (and therefore also of $\mathrm{GL}_2(\mathbb{R})$).

Proposition. $H, K \subset G$ subgroups $\Rightarrow H \cap K \subset G$ is a subgroup.

Proof.
1. As H, K subgroups, $e \in H$ and $e \in K \Rightarrow e \in H \cap K$.
2. $x, y \in H \cap K \Rightarrow x * y \in H$ and $x * y \in K \Rightarrow x * y \in H \cap K$.
3. $x \in H \cap K \Rightarrow x^{-1} \in H$ and $x^{-1} \in K \Rightarrow x^{-1} \in H \cap K$.

□

This result clearly extends to any collection of subgroups of G.

Let $(G, *)$ be a group and let $H \subset G$ be a subgroup. Let us define a relation on G using H as follows:

$$\text{Given } x, y \in G,\ x \sim y \Leftrightarrow x^{-1} * y \in H$$

Proposition 3.14. *This gives an equivalence relation on G.*

Proof. We need to check the three properties of an equivalence relation:

1. (Reflexive)$e \in H \Rightarrow x^{-1} * x \in H \; \forall x \in G \Rightarrow x \sim x$
2. (Symmetric) $x \sim y \Rightarrow x^{-1} * y \in H \Rightarrow (x^{-1} * y)^{-1} \in H \Rightarrow y^{-1} * x \in H \Rightarrow y \sim x$
3. (Transitive) $x \sim y, y \sim z \Rightarrow x^{-1} * y, y^{-1} * z \in H \Rightarrow (x^{-1} * y) * (y^{-1} * z) \in H \Rightarrow x^{-1} * z \in H \Rightarrow x \sim z$

□

Definition. We call the equivalence classes of the above equivalence relation **left cosets** of H in G.

Proposition. For $x \in G$ the equivalence class (or left coset) containing x equals

$$xH := \{x * h \mid h \in H\} \subset G$$

Proof. The easiest way to show that two subsets of G are equal is to prove containment in both directions.

$x \sim y \Leftrightarrow x^{-1} * y \in H \Leftrightarrow x^{-1} * y = h$ for some $h \in H \Rightarrow y = x * h \in xH$. Therefore $\{$Equivalence class containing $x\} \subset xH$.

$y \in xH \Rightarrow y = x * h$ for some $h \in H \Rightarrow x^{-1} * y \in H \Rightarrow y \sim x$. Therefore $xH \subset \{$Equivalence class containing $x\}$. □

This has the following very important consequence:

Corollary 3.15. *Hence for $x, y \in G$, $xH = yH \Leftrightarrow x^{-1} * y \in H$.*

Proof. By the above proposition we know that $xH = yH \Leftrightarrow x \sim y \Leftrightarrow x^{-1} * y \in H$. □

It is very important you understand and remember this fact. An immediate consequence is that $y \in xH \Rightarrow yH = xH$. Hence left cosets can in general be

written with different representatives at the front - **just like an equivalence class modulo n can be written with many different representatives**. This is very important.

Also observe that the equivalence class containing $e \in G$ is just H. Hence the only equivalence class which is a subgroup H, as no other contains the identity. If $H = \{e\}$ then the left cosets are singleton sets.

Remark 3.16. Let $G = \mathbb{R}^3$, thought of as a group under addition. Let H is a two dimensional subspace. Recall this is a subgroup under addition. Geometrically H is a plane which contains the origin. Geometrically the left cosets of H in $\mathbb{R}^3$ are the planes which are parallel to H.

Definition 3.17. Let $(G, *)$ be a group and $H \subset G$ a subgroup. We denote by G/H the set of left cosets of H in G. If the size of this set is finite then we say that H has **finite index** in G. In this case we write

$$(G : H) = |G/H|,$$

and call it the index of H in G.

For $m \in \mathbb{N}$, the subgroup $m\mathbb{Z} \subset Z$ has index m. Note that $\mathbb{Z}/m\mathbb{Z}$ is naturally the set of residue classes modulo m previously introduced. The vector space example in the above remark is not finite index as there are infinitely many parallel planes in $\mathbb{R}^3$

Proposition 3.18. *Let $x \in G$. The map (of sets)*

$$\begin{array}{rcl} \phi : H & \longrightarrow & xH \\ h & \longrightarrow & x * h \end{array}$$

is a bijection.

Proof. We need to check that ϕ is both injective and surjective. For injectivity observe that for $g, h \in H$, $\phi(h) = \phi(g) \Rightarrow x * h = x * g \Rightarrow h = g$. Hence ϕ is injective. For surjectivity observe that $g \in xH \Rightarrow \exists h \in H$ such that $g = x * h \Rightarrow g = \phi(h)$. □

Now let's restrict to the case where G is a finite group.

Proposition. Let $(G, *)$ be a finite group and $H \subset G$ a subgroup. Then $\forall x \in G$, $|xH| = |H|$.

Proof. We know that there is a bijection between H and xH. Both must be finite because they are contained in a finite set. A bijection exists between two finite sets if and only if they have the same cardinality. □

Lagrange's Theorem. Let $(G, *)$ be a finite group and $H \subset G$ a subgroup. Then $|H|$ divides $|G|$.

Proof. We can use H to define the above equivalence relation on G. Because it is an equivalence relation, its equivalence classes cover G and are all disjoint. Recall that this is called a partition of G.

We know that each equivalence class is of the form xH for some (clearly non-unique in general) $x \in G$. We know that any left coset of H has size equal to $|H|$. Hence we have partitioned G into subsets each of size $|H|$. We conclude that $|H|$ divides $|G|$. □

This is a powerful result. It tightly controls the behavior of subgroups of a finite group. For example:

Corollary 3.19. *Let $p \in \mathbb{N}$ be a prime number. Let $(G, *)$ be a finite group of order p. Then the only subgroups of G are G and $\{e\}$.*

Proof. Let H be a subgroup of G. By Lagrange $|H|$ divides p. But p is prime so either $|H| = 1$ or $|H| = p$. In the first case $H = \{e\}$. In the second case $H = G$. □

3.3 Generating Sets for Groups

Definition. Let G be a group and $X \subset G$ be a subset. We define the **subgroup generated by X** to be the intersection of all subgroups of G containing X. We denote it by $\text{gp}(X) \subset G$.

Remark 3.20. 1. $\text{gp}(X)$ is the minimal subgroup containing X. By minimal we mean that if $H \subset G$ is a subgroup such that $X \subset H$ then $gp(X) \subset H$.

2. A more constructive way of defining $\text{gp}(X)$ is as all possible finite compositions of elements of X and their inverses. I leave it as an exercise to check that this subset is indeed a subgroup.

3. Let us consider the group $(\mathbb{Z}, +)$ and $X = \{1\} \subset \mathbb{Z}$. Then $\text{gp}(X)$=$\mathbb{Z}$. This is the precise sense in which $\mathbb{Z}$ is "generated" by 1 under addition.

Definition 3.21. We say that a subset $X \subseteq X$ **generates** a group $(G, *)$ if $\text{gp}(X)$=G.

Definition. We say a group $(G, *)$ is **finitely generated** if it is generated by a finite subset.

Remark 3.22. 1. Clearly all finite groups are finitely generated.

2. The group $(\mathbb{Z}, +)$ is also finitely generated, even though $\mathbb{Z}$ is infinite.

3. The fact that there are infinitely many primes implies that $(\mathbb{Q}\backslash\{0\}, \times)$ is **not** finitely generated.

Definition 3.23. A group $(G, *)$ is said to be cyclic if $\exists x \in G$ such that $gp(\{x\}) = G$, i.e. G can be generated by a single element. In concrete terms this means that $G = \{x^n \mid n \in \mathbb{Z}\}$.

By the above observations $(\mathbb{Z}, +)$ and $(\mathbb{Z}/m\mathbb{Z}, +)$ are examples.

Proposition 3.24. *Any group of prime order is cyclic.*

Proof. Let G be a group of prime order p. Let x be a non-identity element of G. Then $gp(\{x\}) \subset G$ is non-trivial and by Lagrange's theorem must have order p. Hence $G = gp(\{x\})$. □

Remark 3.25. It is important to understand that not all groups are cyclic. We'll see many examples throughout the course.

Let G be a group (not necessarily cyclic). For $r, s \in \mathbb{Z}$ and $x \in G$, $x^r x^s = x^{r+s} = x^{s+r} = x^s x^r$. Hence $gp(\{x\}) \subset G$ is Abelian. We deduce that all cyclic groups are Abelian.

Theorem. Let G be a cyclic group. Then

1. If G is infinite, $G \cong (\mathbb{Z}, +)$
2. If $|G| = m \in \mathbb{N}$, then $G \cong (\mathbb{Z}/m\mathbb{Z}, +)$

Proof. We have two cases to consider.

1. If $G = gp(\{x\})$, then $G = \{\cdots x^{-2}, x^{-1}, e, x, x^2 \cdots\}$. Assume all elements in this set are distinct, then we can define a map of sets:

$$\begin{aligned} \phi : G &\rightarrow \mathbb{Z} \\ x^n &\rightarrow n \end{aligned}$$

   Then,$\forall a, b \in \mathbb{Z}, \phi(x^a * x^b) = \phi(x^{a+b}) = a + b = \varphi(x^a) + \varphi(x^b)$ so φ is a homomorphism which by assumption was bijective. Thus, $(G, *)$ is isomorphic to $(\mathbb{Z}, +)$.

2. Now assume $\exists a, b \in \mathbb{Z}, b > a$ such that $x^a = x^b$. Then $x^{(b-a)} = e \Rightarrow x^{-1} = x^{(b-a-1)} \Rightarrow G = \{e, \cdots, x^{b-a-1}\}$. In particular G is finite. Choose minimal $m \in \mathbb{N}$ such that $x^m = e$. Then $G = \{e, x, \cdots, x^{m-1}\}$ and all its elements are distinct by minimality of m. Hence $|G| = m$.

Define the map

$$\begin{aligned} \phi : G &\rightarrow \mathbb{Z}/m\mathbb{Z} \\ x^n &\rightarrow [n] \text{ for } n \in \{0, ...m-1\} \end{aligned}$$

This is clearly a surjection, hence a bijection because $|G| = |\mathbb{Z}/m\mathbb{Z}| = m$. Again $\forall a, b \in \{0, ..., m-1\}$ we know $\phi(x^a * x^b) = \phi(x^{a+b}) = [a+b] = [a]+[b] = \varphi(x^a)+\varphi(x^b)$ is a homomorphism. Hence $(G, *)$ is isomorphic to $(\mathbb{Z}/m\mathbb{Z}, +)$.

□

Hence two finite cyclic groups of the same size are isomorphic. What are the possible subgroups of a cyclic group?

Proposition. A subgroup of a cyclic group is cyclic.

Proof. If H is trivial we are done. Hence assume that H is non-trivial. By the above we need to check two cases.

1. $(G, *) \cong (\mathbb{Z}, +)$. Let $H \subset \mathbb{Z}$ be a non-trivial subgroup. Choose $m \in \mathbb{N}$ minimal such that $m \in H (m \neq 0)$. Hence $m\mathbb{Z} = \{ma \mid a \in \mathbb{Z}\} \subseteq H$. Assume $\exists n \in H$ such that $n \notin m\mathbb{Z}$. By the remainder theorem, $n = qm + r, r, q \in \mathbb{Z}$ and $0 < r < m \Rightarrow r \in H$. This is a contradiction by the minimality of m. Therefore $m\mathbb{Z} = H$. Observe that $gp(\{m\}) = m\mathbb{Z} \subset \mathbb{Z}$. Hence H is cylic.

2. $(G, *) \cong (\mathbb{Z}/m\mathbb{Z}, +)$. Let $H \subset \mathbb{Z}/m\mathbb{Z}$ be a non-trivial subgroup. Again, choose $n \in \mathbb{N}$ minimal and positive such that $[n] \in H$. The same argument as above shows that the containment $gp(\{[n]\}) \subseteq H$ is actually equality. Hence H is cyclic.

□

Proposition 3.26. *Let $(G, *)$ be a finite cyclic group of order d. Let $m \in \mathbb{N}$ such that m divides $|G|$. Then there is a unique cyclic subgroup of order m.*

Proof. Because $|G| = d$ we know that $G \cong (\mathbb{Z}/d\mathbb{Z}, +)$. Hence we need only answer the question for this latter group. Let m be a divisor of d. Then if $n = d/m$ then $gp(\{[n]\}) \subset \mathbb{Z}/d\mathbb{Z}$ is cyclic of order m by construction. If $H \subset \mathbb{Z}/d\mathbb{Z}$ is a second subgroup of order m then by the above proof we

know that the minimal $n \in \mathbb{N}$ such that $[n] \in H$ must be $n = d/m$. Hence $H = gp(\{[n]\})$.

□

Let $(G, *)$ be a group (not necessarily cyclic) and $x \in G$. We call $gp(\{x\}) \subset G$ the **subgroup generated by x**. By definition it is cyclic.

Definition 3.27. If $|gp(\{x\})| < \infty$ we say that x is of finite order and its order, written $ord(x)$ equals $|gp(\{x\})|$. If not we say that x is of infinite order.

Remark 3.28.

1. Observe that by the above we know that if $x \in G$ is of finite order, then

$$ord(x) = \text{minimal } m \in \mathbb{N} \text{ such that } x^m = e$$

2. $e \in G$ is the only element of G of order 1
3. For $n \in \mathbb{Z}$, if $x^m = e$, then $ord(x)$ divides m. This essentially follows by the second part of the theorem, because n is congruent to 0 modulo $ord(x)$ if and only if it's divisible by $ord(x)$.
4. The only element with finite order in $\mathbb{Z}$ is 0.

Proposition 3.29. *Let $(G, *)$ be a finite group and $x \in G$. Then $ord(x)$ divides $|G|$ and $x^{|G|} = e$.*

Proof. By definition $ord(x) = |gp(\{x\})|$. Therefore, by Lagrange's theorem, $ord(x)$ must divide $|G|$. Also note that by definition $x^{ord(x)} = e$. Hence

$$x^{|G|} = x^{(ord(x) \times \frac{|G|}{ord(x)})} = e^{\frac{|G|}{ord(x)}} = e.$$

□

3.4 Permutation Groups and Finite Symmetric Groups

Definition. Let S be a set. We define **the group of permutations of S** to be the set of **bijections** from S to itself, denoted $\Sigma(S)$, where the group binary operation is **composition of functions**.

Remark 3.30.

1. By composition of functions we always mean on the left, i.e. $\forall f, g \in \Sigma(S)$ and $s \in S$ $(f * g)(s) = f(g(s))$.
2. Associativity clearly has to hold. The identity element e of this group is the identity function on S, i.e. $\forall x \in S$, $e(s) = s$. Inverses exist because any bijective map from a set to itself has an inverse map.
3. Let $n \in \mathbb{N}$. We write $Sym_n := \Sigma(\{1, 2, ..., n\})$. If S is any set of cardinality n then $\Sigma(S)$ is isomorphic to Sym_n, the isomorphism being induced by writing a bijection from S to $\{1, 2, ..., n\}$. We call these groups the finite symmetric groups.
4. Observe that given $\sigma \in \Sigma(S)$ we can think about σ as "moving" S around. In this sense the group $\Sigma(S)$ naturally "acts" on S, and what σ does its called its **action**. The word "action" here will be made more precise in Section 3.5.
5. If $\sigma, \tau \in \Sigma(S)$, we often write $\sigma\tau$ to denote $\sigma \circ \tau$. I.e., as for groups in general, we leave out the group operation, but **it is understood that the group operation is composition of functions**.

The symmetric groups Sym_n give lots of good examples of finite groups (both themselves, and, as we shall see later, some of their subgroups). They also give a bunch of examples of non-abelian groups besides groups of matrices. Let's study them in detail.

I recommend that you also read Section 5.1 of Judson's book.

3.4.1 Active vs. Passive Notation for Permutations

Before we go on, I need to tell you that there are two different ways to write the same permutation, and that can lead to some confusion.

Recall that a permutation of a set S is a bijection from S to itself. So let $S = \{1, 2, 3\}$, and let σ be a permutation for which $\sigma(1) = 2$, $\sigma(2) = 3$, and $\sigma(3) = 1$. Thus $\sigma \in Sym_3$. We often represent σ by the notation (123).

We can think of σ as sending 1 to 2, sending 2 to 3, and sending 3 to 1. We might therefore represent σ as follows:

$$\begin{array}{rcl} & 1 & \longrightarrow & 2 \\ \sigma: & 2 & \longrightarrow & 3 \\ & 3 & \longrightarrow & 1 \end{array}$$

In general, if f is a function such that $f(A) = B$, then we write $A \longrightarrow B$. This justifies the notation. Another way to write the same permutation is

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

We refer to the beginning of Chapter 5 of Judson for this notation.

Writing down all of these arrows is a bit cumbersome. So it's easier to refer to a permutation by a *sequence* of numbers. Notice that from the notation above we get the sequence $2, 3, 1$. So it would seem that the sequence $2, 3, 1$ is a good way to represent this permutation.

HOWEVER, using the sequence $2, 3, 1$ to refer to σ is known as *passive notation*.

Here's a different way to think of it. The fact that $\sigma(1) = 2$ suggests that we should *move* 1 to the place of 2. Similarly, we should *move* 2 to where 3 was, and move 3 to where 1 was.

This gives the sequence $3, 1, 2$, representing the same permutation. This is *active notation*. The distinction between active and passive is discussed in `https://en.wikiversity.org/wiki/Permutation_notation#Active_vs._passive`.

We will primarily use passive notation via the unambiguous notation $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, and because this is in Judson.

However, one has to be extra careful either way when composing two permutations. Let's also consider $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, and let's try to understand $\tau\sigma$. As explained in Remark 3.30.1, this means that we first apply σ and then apply τ.

First, let's find $\tau\sigma$ carefully by thinking of τ and σ as function. We have $\sigma(1) = 2$, $\sigma(2) = 3$, and $\sigma(3) = 1$. Thus $\tau(\sigma(1)) = \tau(2) = 3$, $\tau(\sigma(2)) = \tau(3) = 2$, and $\tau(\sigma(3)) = \tau(1) = 1$. We therefore find that $\tau\sigma$ is the permutation

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

also known as (13), that switches 1 and 3.

Let's see what happens when we think about σ and τ in active notation. We apply σ to get the sequence $3, 1, 2$. Then, when we wish to apply $\tau = (23)$ to the sequence $3, 1, 2$, there is some ambiguity. Do we switch the *numbers* 3 and 2, to get $2, 1, 3$, or do we switch the *numbers in the second and third places* to get $3, 2, 1$? Since we know the answer should give us $3, 2, 1$, it turns out that *when applying a permutation to a sequence in active notation, the permutation* (23) *switches whatever is in the second and third places.*

On the other hand, if we write σ in passive notation, we get $2, 3, 1$, then τ means that we switch *the numbers* 2 *and* 3*, wherever they now appear.*

This issue is discussed at `https://gowers.wordpress.com/2011/10/16/permutations/`, which uses passive and not active notation. If you use active notation, you have to do the opposite of what Gowers writes.

IN CONCLUSION: The best way to be careful is to think of permutations as functions and to compose the functions. But if you want to think of permutations as sequences, then you have to be consistent when composing permutations.

Remark 3.31. Notice that the active notation for σ^{-1} is $2, 3, 1$, and the passive notation for σ^{-1} is $3, 1, 2$. This is not an accident. In general, for ANY permutation σ, the active notation for σ^{-1} is the passive notation for σ, and vice versa.

One important consequence of this is that if σ has order 2 (which is equivalent to saying that $\sigma = \sigma^{-1}$, then the active and passive notations for σ are the same. This is the case for τ above.

3.4.2 The Symmetric Group Sym_3

Let's first discuss the simplest example of a non-abelian symmetric group, which is Sym_3.

One kind of element of Sym_3 is a *transposition*, which switches or "transposes" two numbers. For example, we have the transposition $\sigma = (12)$, which switches 1 and 2:

$$\begin{array}{rcl} & 1 & \longrightarrow & 2 \\ \sigma: & 2 & \longrightarrow & 1 \\ & 3 & \longrightarrow & 3 \end{array}$$

The notation "(12)" shouldn't be hard to understand, although we will explain it in general soon.

We similarly have the transposition (23) and (13).

In addition to transpositions, there are what are known as 3-*cycles*. One example is $\sigma = (123)$

$$\begin{array}{rcl} & 1 & \longrightarrow & 2 \\ \sigma: & 2 & \longrightarrow & 3 \\ & 3 & \longrightarrow & 1 \end{array}$$

We also have the 3-cycle (132):

$$\sigma : \begin{array}{rcl} 1 & \longrightarrow & 3 \\ 2 & \longrightarrow & 1 \\ 3 & \longrightarrow & 2 \end{array}$$

Note that (321) and (213) refer to the same thing as (132). Similarly, (123) = (231) = (312).

Thus far we have listed five elements of Sym_3, namely, $(12), (23), (13), (123), (132)$. We expect there to be $3! = 6$ in total. The one element we have not listed is the *identity*. It is the identity both in the sense that it is the identity function from $\{1, 2, 3\}$ to itself, and in that it is the identity of the group Sym_3. We denote the identity either by e or by (1) (or (2) or (3) are equally good notation).

Now that we've listed some elements of Sym_3, let's talk about the group operation. As described above, the group operation is just composition of functions. Let's give an example to make sure it's clear

Let's say $\sigma = (123)$ and $\tau = (23)$. Let's find $\tau\sigma$. As explained in Section 3.4.1, this is (13).

What about $\sigma\tau$? Applying τ, one gets $1, 3, 2$, and then applying σ, one gets $2, 1, 3$, which in total is the same as applying (12). Thus $\sigma\tau = (12)$. Notice that this is not the same as $\tau\sigma$, so they do not commute.

3.4.3 Symmetric Groups in General

The most basic property of a finite group is how many elements it has (also known as its *order*). Let's see what this is for Sym_n.

Proposition 3.32. *For $n \in \mathbb{N}$, $|Sym_n| = n!$.*

Proof. Any permutation σ of $\{1, 2...n\}$ is totally determined by a choice of $\sigma(1)$, then $\sigma(2)$ and so on. At each stage the possibilities drop by one. Hence the number of permutations is $n!$. □

We need to think of a way of elegantly representing elements of Sym_n. For $a \in \{1, 2...n\}$ and $\sigma \in Sym_n$ we represent the action of σ on a by a cycle. For example, we represent a 6-cycle as:

$$(abc...f) \text{ where } b = \sigma(a),\ c = \sigma(b)...\sigma(f) = a.$$

Note that a, b, c, d, e, f can be any elements of the set $\{1, 2, \cdots, n\}$, and they *don't* have to be in order. In general, we define:

Definition 3.33. If S is a set, and $a_1, a_2, \cdots, a_k$ is sequence of distinct elements of S, then the k-cycle

$$\sigma = (a_1 a_2 \cdots a_k)$$

is the element of $\Sigma(S)$ such that $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3$, $\cdots$, $\sigma(a_{k-1}) = a_k$, $\sigma(a_k) = a_1$, and $\sigma(a) = a$ whenever a is NOT in the finite set $\{a_1, \cdots, a_k\}$.

Remark 3.34.

1. A k-cycle always has order k.
2. There are exactly k different ways to write a given k-cycle. For example, $(123) = (231) = (312) \in Sym_3$.
3. A 1-cycle is the same as id_S.

We are going to explain how to write every permutation as a product of cycles in an essentially unique way, known as disjoint cycle notation. For this, we need to explain what disjoint means, and before we explain what disjoint means, we need a couple of definitions:

Definition 3.35. Let S be a set and $\sigma \in \Sigma(S)$. Then we define

$$Fixed(\sigma) \coloneqq \{s \in S \mid \sigma(s) = s\}.$$

Note that $Fixed(\sigma)$ is a subset of S.

Notice that $Fixed(\sigma) = S$ iff $\sigma = id_S$.

If $\sigma = (a_1 a_2 \cdots a_k)$ is a k-cycle, for $k \geq 2$, then $Fixed(\sigma) = S \backslash \{a_1, \cdots, a_k\}$.

Here is a related definition:

Definition 3.36. Let S be a set and $s \in S$. Then we define

$$Fix(s) \coloneqq \{\sigma \in \Sigma(S) \mid \sigma(s) = s\}.$$

Note that $Fix(s)$ is a subset of $\Sigma(S)$. It is clearly a subset of $\Sigma(S)$. In fact, it is a subgroup, which we will prove in Section 3.5.1. It is also called the *stabiliser subgroup of* s.

Notice that $s \in Fixed(\sigma)$ iff $\sigma \in Fix(s)$. In this case, we say that σ *fixes* s.

We can now define what it means to be disjoint:

Definition 3.37. If $\sigma, \tau \in \Sigma(S)$, then we say that σ and τ are *disjoint* if $Fixed(\sigma) \cup Fixed(\tau) = S$. In other words, every element of S is either fixed by σ or fixed by τ.

Proposition 3.38. *If σ, τ are disjoint, then $\sigma\tau = \tau\sigma$.*

Proof. We need to show that for every $s \in S$, we have $\sigma(\tau(s)) = \tau(\sigma(s))$.

First, suppose that $s \in Fixed(\sigma)$. Then $\tau(\sigma(s)) = \tau(s)$. Then either $\tau(s) \in Fixed(\sigma)$, or $\tau(s) \in Fixed(\tau)$. In the first case, we have $\sigma(\tau(s)) = \tau(s) = \tau(\sigma(s))$, so we are done. In the second case, we have $\tau(\tau(s)) = \tau(s)$. Applying τ^{-1} to both sides, we find that $\tau(s) = s$. This implies that $\sigma(\tau(s)) = \sigma(s) = s = \tau(s) = \tau(\sigma(s))$, so we are done.

Next, suppose that $s \in Fixed(\tau)$. We can similarly reason based on whether $\sigma(s) \in Fixed(\sigma)$ or $\sigma(s) \in Fixed(\tau)$. The proof in this case is the same. □

Since Sym_n is finite, every element has finite order by Proposition 3.29. We know that eventually we get back to a because σ has finite order. Thus σ eventually takes everything back to where it started. In this way every $\sigma \in Sym_n$ can be written as a product of disjoint cycles:

$$\sigma = (a_1 ... a_r)(a_{r+1} ... a_s) ... (a_{t+1} ... a_n).$$

This representation is unique up to internal shifts and reordering the cycles. We will give a detailed example of this in Example 3.40.

E.g. Let $n = 5$ then $\sigma = (123)(45)$ corresponds to

$$\begin{array}{rcl} & 1 & \longrightarrow & 2 \\ & 2 & \longrightarrow & 3 \\ \sigma : & 3 & \longrightarrow & 1 \\ & 4 & \longrightarrow & 5 \\ & 5 & \longrightarrow & 4 \end{array}$$

If an element is fixed by σ we omit it from the notation.

E.g. Let $n = 5$ then $\sigma = (523)$ corresponds to

$$\begin{array}{rcl} & 1 & \longrightarrow & 1 \\ & 2 & \longrightarrow & 3 \\ \sigma : & 3 & \longrightarrow & 5 \\ & 4 & \longrightarrow & 4 \\ & 5 & \longrightarrow & 2 \end{array}$$

This notation makes it clear how to compose two permutations. For example, let $n = 5$ and $\sigma = (23), \tau = (241)$, then $\tau\sigma = (241)(23) = (1234)$ and $\sigma\tau = (23)(241) = (1324)$. Observe that composition is on the left when composing permutations. This example also shows that in general Sym_n is not Abelian.

Hence, given $\sigma \in Sym_n$, we naturally get a well-defined partition of n, taking the lengths of the disjoint cycles appearing in σ. This is call the **cycle structure** of σ. In other words, if we can write

$$\sigma = \sigma_1\sigma_2 \cdots \sigma_m,$$

where σ_i is a k_i-cycle, and $\sum_i k_i = n$, and the σ_i are all disjoint, then the cycle structure is $\{k_1, \cdots, k_m\}$. Note that the k_i need not be all distinct, and

we usually write them in ascending order. The number of k_i's equal to 1 is just the size of $Fixed(\sigma)$.

Proposition 3.39. *Let $\sigma \in Sym_n$ have cycle structure $\{n_1, \cdots, n_m\}$. Then $ord(\sigma) = LCM(n_1, ...n_m)$, where LCM denotes the lowest common multiple.*

Proof. Let $\sigma = (a_1, \cdots, a_r)(a_{r+1}, \cdots, a_s) \cdots (a_{t+1}, \cdots, a_n)$, be a representation of σ as the disjoint product of cycles. We may assume that $r = n_1$, etc, without any loss of generality. Observe that a cycle of length $d \in \mathbb{N}$ must have order d in Sym_n. Also recall that if G is a finite group then for any $d \in \mathbb{N}$, $x \in G$, $x^d = e \Leftrightarrow ord(x) \mid d$. Also observe that for all $d \in \mathbb{N}$, $\sigma^d = (a_1, \cdots, a_r)^d (a_{r+1}, \cdots, a_s)^d \cdots (a_{t+1}, \cdots, a_n)^d$, because disjoint cycles commute by Proposition 3.38. Thus we know that $\sigma^d = e \Leftrightarrow n_i \mid d \; \forall i$. The smallest value d can take with this property is $LCM(n_1, ...n_m)$. □

Example 3.40. Let's give an example of how you would write a permutation in disjoint cycle notation. For example, suppose we have the following element of Sym_9:

$$\begin{array}{rcl} & 1 & \longrightarrow & 5 \\ & 2 & \longrightarrow & 1 \\ & 3 & \longrightarrow & 7 \\ & 4 & \longrightarrow & 3 \\ \sigma: & 5 & \longrightarrow & 2 \\ & 6 & \longrightarrow & 6 \\ & 7 & \longrightarrow & 9 \\ & 8 & \longrightarrow & 8 \\ & 9 & \longrightarrow & 4 \end{array}$$

We start by seeing where 1 goes. We get $\sigma(1) = 5$, $\sigma(\sigma(1)) = 2$, and finally $\sigma^3(1) = 1$. So that means that 1 travels to 5, then to 2, then back to 1, so we get the cycle (152) as one of the disjoint cycles making up σ.

Next, we see what happens to 2. But aha! We already had 2 appear in a cycle. So there's no point in considering it, and we move on to 3.

For 3, we see what happens when we keep applying σ. We get $\sigma(3) = 7$, $\sigma^2(3) = 9$, $\sigma^3(3) = 4$, and finally $\sigma^4(3) = 3$ again. So 3 goes to 7, then to 9, then to 4, then back to 3. In other words, we have another cycle (3794).

We can ignore 4, as it appears in (3794), and we can ignore 5, as it already appears in (152). But when we get to 6, we notice that it doesn't appear in any of the cycles we already wrote down. In fact, 6 is fixed by σ, so 6 is in a 1-cycle, (6). Of course, because all 1-cycles are the identity, we don't actually need to write it in the disjoint cycle decomposition.

Finally, the only number left out is 8, and like with 6, we have $\sigma(8) = 8$.

Thus the disjoint cycle notation for σ is (152)(3794). Note that we could also write (152)(3794)(6)(8), if we want to remember the 1-cycles, but we usually leave them out. The one good thing about including the one-cycles is that it helps you write the cycle structure: in this case, the cycle structure is $\{1, 1, 3, 4\}$.

Let's also see what Proposition 3.39 says in this case. The order must be $LCM(1, 1, 3, 4) = 12$.

As mentioned, the disjoint cycle notation for σ is unique, but only up to internal shifts and reordering the cycles. Notice that (152) = (521) = (215), and (3794) = (7943) = (9437) = (4379) (as mentioned above, there are k ways to write a k-cycle). This gives (3)(4) = 12 different ways to write the disjoint cycle notation. In fact, there are 2 different ways to order these disjoint cycles, so we have 24 different ways to write the disjoint cycle notation.

It's fine to write a given permutation's disjoint cycle notation in whichever way you want. The important thing to understand is that disjoint cycle notation is unique only up to internal shifts and reordering the cycles.

This is similar to how prime factorization is "unique," but only up to reordering the prime factors.

Definition 3.41. A **transposition** is a cycle of length 2.

Observe that we can write any cycle as a product of transpositions:

k

Hence any permutation $\sigma \in \mathrm{Sym}_n$ may be written as the (not necessarily disjoint) product of transpositions. This representation is non-unique as the following shows:

e.g. n=6, σ=(1 2 3)=(1 3) (1 2)=(4 5)(1 3)(4 5)(1 2)

Notice that both expressions involve an even number of transpositions.

Theorem. Let $\sigma \in \mathrm{Sym}_n$ be expressed as the product of transpositions in two potentially different ways. If the first has m transpositions and the second has n transpositions then $2 \mid (m - n)$.

Proof. First notice that a cycle of length r can be written as the product of $r - 1$ transpositions by the above. Let us call σ even if there are an even number of even length cycles (once expressed as a disjoint product); let us call σ odd if there are an odd number of even length cycles. We also define the sign of σ, denoted $sgn(\sigma)$, to be $+1$ or -1 depending on whether σ is even or odd.

Consider how sign changes when we multiply by a transposition $(1\ i)$. We have two cases:

1. 1 and i occur in the same cycle in σ. Without loss of generality we consider $(1\ 2 \cdots\ i \cdots\ r)$ as being in σ.

   $$(1\ \mathrm{i})(1\ 2 \cdots\ i \cdots\ r)=(1\ 2 \cdots\ i-1)(i\ i+1 \cdots\ r)$$

   If r is even then either we get two odd length cycles or two even length cycles. If r is odd then exactly one of the cycles on the right is even length. In either case, $sgn((1\ i)\sigma) = -sgn(\sigma)$.

2. 1 and i occur in distinct cycles. Again, without loss of generality we may assume that $(1 \cdots i-1)(i \cdots r)$ occurs in σ. In this case

$$(1\ \mathrm{i})(1\ 2 \cdots\ i-1)(i \cdots\ r)=(1 \cdots\ r).$$

In either of the cases r even or odd, we see that the number of even length cycles must drop or go up by one. Hence $sgn((1\ i)\sigma) = -sgn(\sigma)$ as in case 1.

We deduce that multiplying on the left by a transposition changes the sign of our permutation. The identity must have sign 1, hence by induction we see that the product of an odd number of transpositions has sign -1, and the product of an even number of transpositions has sign 1.

Note that if we write any product of transpositions then we can immediately write down an inverse by reversing their order. Let us assume that we can express σ as the product of transpositions in two different ways, one with an odd number and one with an even number. Hence we can write down σ as the product of evenly many transpositions and σ^{-1} as a product of an odd number of transpositions. Thus we can write $e = \sigma * \sigma^{-1}$ as a product of an odd number of transpositions. This is a contradiction as $sgn(e) = 1$. □

We should observe that from the proof of the above we see that $\forall \sigma, \tau \in Sym_n$, $sgn(\sigma\tau) = sgn(\sigma)sgn(\tau)$. Because $sgn(e) = 1$ we deduce that $sgn(\sigma) = sgn(\sigma^{-1})$ for all $\sigma \in Sym_n$.

In particular this shows that the set of even elements of Sym_n contains the identity and is closed under composition and taking inverse. Hence we have the following:

Definition 3.42. The subgroup of $Alt_n \subset Sym_n$ consisting of even elements is called the Alternating group of rank n.

Observe that Alt_n contains all 3-cycles (cycles of length 3).

Proposition 3.43. *Alt_n is generated by 3-cylces.*

Proof. By generate we mean that any element of Alt_n can be expressed as the product of three cycles. As any element of Alt_n can be written as the product of three cycles we only have to do it for the product of two transpositions. There are two cases:

1. $(i\ j)(k\ l) = (k\ i\ l)(i\ j\ k)$.
2. $(i\ j)(i\ k) = (i\ k\ j)$.

□

Proposition 3.44. $|Alt_n| = \dfrac{n!}{2}$.

Proof. Recall that $|Sym_n| = n!$, hence we just need to show that $(Sym_n : Alt_n) = 2$. Let $\sigma, \tau \in Sym_n$. Recall that

$$\sigma Alt_n = \tau Alt_n \Leftrightarrow \sigma^{-1}\tau \in Alt_n.$$

But $sgn(\sigma^{-1}\tau) = sgn(\sigma)sgn(\tau)$, hence

$$\sigma Alt_n = \tau Alt_n \Leftrightarrow sgn(\sigma) = sgn(\tau).$$

Hence Alt_n has two left cosets in Sym_n, one containing even permutations and one odd permutations. □

Later we shall see that the alternating groups for $n \geq 5$ have a very special property.

3.5 Group Actions

Definition. Let $(G, *)$ be a group and S a set. By a group action of $(G, *)$ on S we mean a homomorphism

$$\varphi \colon G \to \Sigma(S)$$

If the action of the group is understood we will write

$$g(s) = \varphi(g)(s) \,\forall\, g \in G,\ s \in S.$$

Note that $\varphi(g)(s)$ means that $\varphi(g)$ is an element of $\Sigma(S)$, and we *apply* that element of $\Sigma(S)$ to $s \in S$.

Remark 3.45. An action of G on S is the same as a map:

$$\mu : G \times S \to S$$

such that

1. $\forall x, y \in G, s \in S, \mu(x * y, s) = \mu(x, \mu(y, s))$
2. $\mu(e, s) = s$

We also sometimes write ϕ in place of μ (as was done in class).

One can write μ in terms of φ by setting

$$\mu(g, s) = \varphi(g)(s)$$

It is an exercise for you to check that μ then satisfies the axioms listed, and conversely that every such μ corresponds to an action φ.

We will often define actions in terms of μ rather than φ. But the definition in terms of φ is more intuitive for most people.

The notation $g(s) = \mu(g)(s)$ makes the axioms clearer: (1) becomes $(x * y)(s) = x(y(s))\ \forall x, y \in G, s \in S$ and (2) becomes $e(s) = s\ \forall s \in S$.

Example 3.46. 1. Notice that there is a natural action of $\Sigma(S)$ on S:

$$\begin{aligned} \mu : \Sigma(S) \times S &\to S \\ (f, s) &\to f(s) \end{aligned}$$

In terms of φ, this is just the identity homomorphism from $\Sigma(S)$ to itself.

2. Let $(G, *)$ be a group. There is a natural action of G on itself:

$$\begin{aligned} \mu : G \times G &\to G \\ (x, y) &\to x * y \end{aligned}$$

Property (1) holds as $*$ is associative. Property (2) holds because $e * x = x \ \forall x \in G$. This is called the **left regular representation** of G.

3. We define the trivial action of G on S by

$$\begin{aligned} \mu : G \times S &\to S \\ (g, s) &\to s \ \ \forall s \in S, \ g \in G \end{aligned}$$

4. There is a natural action of $\mathrm{GL}_n(\mathbb{R})$ on $\mathbb{R}^n$. If we represent $v \in \mathbb{R}^n$ as a column vector, and $g \in \mathrm{GL}_n(\mathbb{R})$, then we define $\mu(g, v)$ to be the matrix multiplication gv. More generally, if G is any subgroup of $\mathrm{GL}_n(\mathbb{R})$, then we get an action of G on V.

5. There is another natural action of G on itself:

$$\begin{aligned} \mu : G \times G &\to G \\ (x, y) &\to x^* y * x^{-1} \end{aligned}$$

Property (1) holds because of associativity of $*$ and that $(g * h)^{-1} = h^{-1} * g^{-1}$. Property (2) is obvious. This action is called conjugation. We will discuss it in more detail in Section 3.5.2.

Definition 3.47. An action of G on S is called **faithful** if

$$\varphi : G \to \Sigma(S)$$

is injective.

Notice that if G and H are two groups and $f : G \to H$ is an injective homomorphism then we may view G as a subgroup of H by identifying it with its image in H under f. Hence if G acts faithfully on S then G is isomorphic to a subgroup of $\Sigma(S)$.

Cayley's Theorem. Let G be a group. Then G is isomorphic to a subgroup of $\Sigma(G)$. In particular if $|G| = n \in \mathbb{N}$, then G is isomorphic to a subgroup of Sym_n.

Proof. The result will follow if we can show that the left regular representation is faithful. Let $\varphi : G \to \Sigma(G)$ be the homomorphism given by the left regular representation. Hence for $g, s \in G$, $\varphi_g(s) = g * s$. For$h, g \in G$, suppose $\varphi_h = \varphi_g$. Then $h * s = g * s \; \forall s \in G \Rightarrow h = g$. Hence φ is injective.

In particular, if G has n elements, then there is a bijection between G and $\{1, \cdots, n\}$ (in some set theory textbooks, this is the definition of having n elements). It is not hard to see that if two sets S, T are in bijection, then $\Sigma(S)$ and $\Sigma(T)$ are isomorphic. Thus $\Sigma(G)$ is isomorphic to Sym_n, so every subgroup of $\Sigma(G)$ is isomorphic to a subgroup of Sym_n.

□

3.5.1 The Orbit-Stabiliser Theorem

Definition. Let $(G, *)$ be a group, together with an action φ on a set S. We can define an equivalence relation on S by

$$s \sim t \Leftrightarrow \exists g \in G \text{ such that } g(s) = t$$

Remark 3.48. This is an equivalence relation as a consequence of the group axioms, together with the definition of an action. I leave it as an exercise to check this.

Definition 3.49. Let $(G, *)$ be a group, together with an action φ on a set S. Under the above equivalence relation we call the equivalence classes orbits, and we write

$$Orb(s) := \{t \in S \mid \exists g \in G \text{ such that } g(s) = t\} \subset S$$

for the equivalence class containing $s \in S$. We call it the **orbit** of s.

It is important to observe that $Orb(s)$ is a subset of S and hence is merely a set with no extra structure.

Definition 3.50. Let $(G, *)$ be a group, together with an action φ on a set S. We say that G acts **transitively** on S is there is only one orbit. Equivalently, φ is transitive if given $s, t \in S$, $\exists g \in G$ such that $g(s) = t$.

An example of a transitive action is the natural action of $\Sigma(S)$ on S. This is clear because given any two points in a set S there is always a bijection which maps one to the other. If G is not the trivial group (the group with one element) then conjugation is never transitive. To see this observe that under this action $Orb(e) = \{e\}$.

Definition 3.51. Let $(G, *)$ be a group, together with an action φ on a set S. Let $s \in S$. We define the stabiliser subgroup of s to be all elements of G which **fix** s under the action. More precisely

$$Stab(s) = \{g \in G \mid g(s) = s\} \subset G$$

In the special case of $\Sigma(S)$ acting on S, we called this $Fix(s)$.

For this definition to make sense we must prove that $Stab(s)$ is genuinely a subgroup.

Proposition. Stab(s) is a subgroup of G.

Proof.

1. $e(s) = s \Rightarrow e \in Stab(s)$
2. $x, y \in Stab(s) \Rightarrow (x * y)(s) = x(y(s)) = x(s) = s \Rightarrow x * y \in Stab(s)$.
3. $x \in Stab(s) \Rightarrow x^{-1}(s) = x^{-1}(x(s)) = (x^{-1} * x)(s) = e(s) = s \Rightarrow x^{-1} \in Stab(s)$

□

Thus we may form the left cosets of $Stab(s)$ in G:

$$G/Stab(s) := \{xStab(s) \mid x \in G\}.$$

Recall that these subsets of G are the equivalence classes for the equivalence relation:

$$\text{Given } x, y \in G,\ x \sim y \Leftrightarrow x^{-1} * y \in Stab(s),$$

hence they partition G into disjoint subsets.

Proposition 3.52. *Let $x, y \in G$ then xStab(s)=yStab(s)$\Leftrightarrow$ $x(s) = y(s)$.*

Proof. Recall that x and y are in the same left coset $\Leftrightarrow$ $x^{-1}y \in Stab(s)$. Hence $x^{-1}y(s) = s$. Composing both sides with x and simplifying by the axioms for a group action implies that $x(s) = y(s)$. □

We deduce that there is a *well defined* map (of sets):

$$\begin{aligned} \phi : G/Stab(s) &\longrightarrow Orb(s) \\ xStab(s) &\longrightarrow x(s) \end{aligned}$$

Proposition. ϕ is a bijection.

Proof. By definition, $Orb(s) := \{x(s) \in S \mid x \in G\}$. Hence ϕ is trivially surjective.

Assume $\phi(xStab(s)) = \phi(yStab(s))$ for some $x, y \in G$. This implies the following:

$$\begin{aligned} x(s) = y(s) &\Rightarrow x^{-1}(y(s)) = s \\ &\Rightarrow (x^{-1} * y)(s) = s \\ &\Rightarrow x^{-1} * y \in Stab(s) \\ &\Rightarrow xStab(s) = yStab(s) \end{aligned}$$

Therefore ϕ is injective.

□

This immediately gives the following key result:

Orbit-Stabiliser Theorem. Let $(G, *)$ be a group together with an action, φ, on a set S. Let $s \in S$ such that the orbit of s is finite ($|Orb(s)| < \infty$). Then $stab(s) \subset G$ is of finite index and

$$(G : Stab(s)) = |Orb(s)|$$

Proof. Immediate from previous proposition. □

We have the following corollary:

Corollary 3.53. *If $(G, *)$ is a finite group acting on a set S and $s \in S$ then*

$$|G| = |Stab(s)| \cdot |Orb(s)|.$$

Proof. In this case $(G : Stab(s)) = |G|/|Stab(s)|$. Applying the orbit-stabiliser theorem yields the result. □

Here are some examples of orbits and stabilisers:

Example 3.54. 1. If G acts trivially on a set S, then for all $s \in S$, we have $Stab(s) = G$. The orbits are all one-element sets.

2. In the left regular representation, all stabilisers are trivial, i.e. $\{e\}$. This is because if $gx = x$, then $g = e$. The action is transitive, i.e., there is one orbit.

3. In the conjugation action of G on itself, we have $Stab(x) = \{g \in G \mid gx = xg\}$. This is known as the *centraliser* of x and is the topic of Section 3.5.2.

4. In the natural action of $\mathrm{GL}_n(\mathbb{R})$ on $\mathbb{R}^n$, the stabiliser of the unit vector $(1, 0, \cdots, 0)$ is the set of invertible matrices whose first column is

$$\begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

   More generally, the stabiliser of the ith unit vector is the set of invertible $n \times n$ matrices whose ith column is the ith unit vector.

   In all of these cases, the orbit is the set of nonzero elements of $\mathbb{R}^n$.

5. When $G = Sym_n$ acts in the natural way on $S = \{1, \cdots, n\}$, the stabiliser of any $k \in S$ is a subgroup of Sym_n isomorphic to Sym_{n-1}. Note that this agrees with the Orbit-Stabiliser Theorem: the action is transitive, so the orbit of any $k \in S$ is all of S, hence has size n. Thus the stabiliser has size $\dfrac{|Sym_n|}{n} = \dfrac{n!}{n} = (n-1)!$, which is indeed the size of Sym_{n-1}.

6. More specifically, in the previous example, if $n = 2$, then $Stab(1) = \{id, (23)\}$, and $Stab(3) = \{id, (12)\}$.

7. Again referring to the previous example, if $n = 4$, then $Stab(2) = \{id, (13), (14), (34), (134), (143)\}$.

3.5.2 Centralizers and Conjugacy Classes

The Orbit-Stabiliser theorem will allow us to prove non-trivial results about the structure of finite groups (in Section 3.5.3) when we apply it to the action known as *conjugation*. We now discuss the conjugation action in more detail.

For $g \in G$, the map

$$[g] \colon G \to G$$

defined by

$$[g](x) = gxg^{-1}$$

for $x \in G$ is called *conjugation by* g. For a fixed g, this gives a bijection from G to itself (to see that it is bijection, notice that $[g^{-1}]$ gives the inverse bijection). As we let g vary, this defines an action of G on itself.

Given $x \in G$, define the *centralizer* of x in G by

$$C_G(x) = \{g \in G \mid gxg^{-1} = x\}.$$

It is clear from the definition that this is the stabilizer

$$\mathrm{Stab}_G(x)$$

of x under the conjugation action, so $C_G(x)$ must be a subgroup. It is also simply the set of $g \in G$ that commute with x.

So that tells us that $g \in C_G(x)$ if and only if g commutes with x. But that's the same thing as saying that x commutes with g, so it's equivalent to saying that $x \in C_g(x)$. In fact, by that reasoning, we have

$$C_G(x) = \{g \in G \mid x \in C_G(g)\}.$$

Recall the following definition from the homework:

Definition 3.55. Let $(G, *)$ be a group. The center of G is the subset

$$Z(G) := \{h \in G \mid g * h = h * g,\ \forall g \in G\}.$$

It is clear that $Z(G)$ is the intersection of all centralizers, i.e.,

$$Z(G) = \bigcap_{x \in G} C_G(x).$$

Note that the conjugation action is faithful iff the center is trivial, i.e., $Z(G) = \{e\}$.

The following is an important fact about conjugation that distinguishes it from the left regular representation:

Proposition 3.56. *If $g \in G$, then the map*

$$\begin{aligned} \varphi(g)\colon G &\to G \\ x &\mapsto gxg^{-1} \end{aligned}$$

is a homomorphism from G to itself.

Proof. We have

$$\begin{aligned} \varphi(g)(xy) &= gxyg^{-1} \\ &= gxeyg^{-1} \\ &= gxg^{-1}gyg^{-1} \\ &= (gxg^{-1})(gyg^{-1}) \\ &= \varphi(g)(x)\varphi(g)(y), \end{aligned}$$

which shows that $\varphi(g)$ is a homomorphism. Notice that we don't bother writing parentheses for the most part, because the group operation is always associative (but the order does matter!). □

On the other hand, for the left regular representation, notice that $\varphi(g)$ sends e to g, so it can't be a homomorphism from G to itself unless $g = e$.

Thus in the case of the conjugation action, the image of the homomorphism

$$\varphi\colon G \to \Sigma(G)$$

sits inside the subset

$$\mathrm{Aut}(G) \subseteq \Sigma(G)$$

of bijections from G to itself that also happen to be homomorphisms. One implication of this is that every element in the same conjugacy class must have the same order.

The orbit of x under this action is known as the *conjugacy class* of x and is denoted

$$Conj(x) = Orb(x) = \{g^{-1} * x * g \mid g \in G\}.$$

Remark 3.57. The following are equivalent:

- $x \in Z(G)$
- $Conj(x)$ has one element
- $C_G(x) = G$

By the Orbit-Stabilizer Theorem, we know that the size of the conjugacy class of x times the size of $C_G(x)$ is $|G|$ (at least assuming these are finite).

The previous fact is *very important* for computing the centralizer of an element. If you just have some elements that commute with x, then you know you've found some of $C_G(x)$, but it's not clear that you've found *all* of $C_G(x)$. But if you know $|C_G(x)|$, and you've found that many elements that commute with x, then you know you've found all of $C_G(x)$. See, for example, Example 3.60.

Remark 3.58. Since x commutes with all of powers, we always have

$$gp(\{x\}) \subseteq C_G(x).$$

Assuming G is finite, note that $|gp(\{x\})|$ is just the order of x. It follows that $|C_G(x)| \geq \text{ord}(x)$, and thus the conjugacy class of x has size at most $\dfrac{|G|}{\text{ord}(x)}$.

Example 3.59. If G is abelian (for example, $\mathbb{Z}/m\mathbb{Z}$), then $C_G(x) = G$ for every element x, and every conjugacy class has one element. This is the same as saying that the conjugation action is the trivial action.

Example 3.60. As an example, consider $x = (123) \in G = Sym_5$. Then the conjugacy class of x is the set of all 3-cycles. To count the number of three-cycles, notice that there are $\binom{5}{3} = 10$ ways to choose the three elements

that are cycled, and there are two cycles for each triple (think about how (123) and (132) are different elements of Sym_5), so there are 20 three-cycles. Since $|Sym_5| = 5! = 120$, the size of $C_G(x)$ must be $120/20 = 6$.

What are these six elements? We can take the subgroup generated by (123)(45). Notice that this element has order 6 (as it's the LCM of 2 and 3) and is in $C_G(x)$, so it must in fact generate all of $C_G(x)$.

Example 3.61. For $G = Sym_3$, the conjugacy classes are $\{\text{id}\}$, $\{(12), (23), (31)\}$, and $\{(123), (132)\}$. Since $|G| = 6$, the stabilizer of id is G, the centralizer of (12) has two elements, and the centralizer of (123) has three elements. In fact, in the latter two cases, the centralizer of the element is just the subgroup it generates (so the inclusion in Remark 3.58 is in fact an equality of subgroups in these cases).

In fact, in general, there is a simple description of the conjugacy classes in Sym_n. We begin with a lemma.

Lemma 3.62. *If $\sigma \in Sym_n$ is the k-cycle*

$$(s_1 \cdots s_k),$$

and $\alpha \in Sym_n$ is any element, then

$$\alpha\sigma\alpha^{-1} = (\alpha(s_1) \cdots \alpha(s_k)),$$

i.e., it is still a k-cycle.

Theorem 3.63. *Two permutations are conjugate in Sym_n if and only if they have the same cycle structure.*

Proof. Let $\sigma, \tau \in Sym_n$ have the same cycle structure $\{k_1, \cdots, k_r\}$. Hence we may represent both in the form:

$$\sigma = \sigma_1\sigma_2 \cdots \sigma_r,$$

$$\tau = \tau_1\tau_2 \cdots \tau_r,$$

where σ_i is a k_i-cycle, and $\sum_{i=1}^{r} k_i = 1$. Write

$$\sigma_i = (a_{i1} \cdots a_{ik_i})$$

$$\tau_i = (b_{i1} \cdots b_{ik_i})$$

for $i = 1, 2, \cdots, r$. Define $\alpha \in Sym_n$ such that $\alpha(a_{ij}) = b_{ij}$ for all $1 \leq i \leq r$, $1 \leq j \leq k_i$. Then by Lemma 3.62, we have

$$\alpha\sigma_i\alpha^{-1} = \tau_i$$

for each i. Since conjugation by α is an automorphism of Sym_n (and hence a homomorphism), we get

$$\alpha\sigma\alpha^{-1} = \tau.$$

Conversely, if α is any element of Sym_n, and

$$\sigma = \sigma_1\sigma_2 \cdots \sigma_r,$$

then

$$\alpha\sigma_i\alpha^{-1}$$

is a k_i-cycle for each i by Lemma 3.62, and they are all disjoint (because α is a bijection), so $\alpha\sigma\alpha^{-1}$ has the same cycle structure as σ.

□

Corollary 3.64. *Conjugacy classes in Sym_n are indexed by cycle structures (i.e. partitions of n).*

Proof. Immediate from the above. □

Thus the number of conjugacy classes in Sym_n is the number of partitions of n, often denoted $p(n)$. To learn more about $p(n)$, see `https://en.wikipedia.org/wiki/Partition_function_(number_theory)`.

Example 3.65. For $G = Sym_4$, the conjugacy classes are $\{\text{id}\}$, $\{(12), (23), (34), (41), (13), (24)\}$, $\{(123), (132), (124), (142), (134), (143), (234), (243)\}$, $\{(1234), (1243), (1324), (1342), (1423), (1432)\}$ and $\{(12)(34), (13)(24), (14), (23)\}$.

The centralizer of id is G, as always.

The centralizer of (12) must have four elements, as its conjugacy class has $24/4 = 6$ elements. Recall that disjoint cycles don't commute, so (34) is in $C_G((12))$. As well, by Remark 3.58, we know that $(12) \in C_G((12))$. So we have $C_G((12)) = \{\text{id}, (12), (34), (12)(34)\}$.

Notice that the conjugacy class of (123) has eight elements, so its centralizer has $24/8 = 3$ elements. In fact, it has order 3, so its centralizer is just the subgroup it generates. Similarly, the conjugacy class of (1234) has six elements, so its centralizer has 4 elements, and it has order 4, so it must generate its centralizer.

Finally, note that the conjugacy class of (12)(34) has three elements, so its centralizer must have eight elements. Recall that (12)(34) commutes with the cycles (12) and (34), so it commutes with the subgroup they generate, i.e., $\{\text{id}, (12), (34), (12)(34)\}$. Finally, more subtle is the fact that (13)(24) also commutes with (12)(34). Note carefully that (13) and (24) do NOT commute with it. We can then take the subgroup generated by (13)(24) and $\{\text{id}, (12), (34), (12)(34)\}$, and this indeed has eight elements so it is the centralizer.

Example 3.66. If $G = GL_n(\mathbb{R})$, the group of invertible $n \times n$ matrices with real entries (under matrix multiplication), then two matrices are in the same conjugacy class if and only if they are similar, or equivalently, have the same Jordan normal form. Note in particular that any two conjugate matrices have the same eigenvalues and characteristic polynomial.

We end with a nice little fact about conjugation and stabilisers:

Fact 3.67. Let G act on a set S, let $x, y \in S$, and suppose $\tau \in G$. If $\tau(x) = y$, then

$$\sigma \in Stab(x)$$

if and only if

$$\tau\sigma\tau^{-1} \in Stab(y).$$

In particular, elements of $Stab(x)$ are conjugate to elements of the stabiliser of any element of the orbit of x.

3.5.3 Sylow's Theorem

We start with a remark that will help us prove Theorem 3.69. This will be our first example of a non-trivial theorem that uses the theory of conjugacy classes.

Remark 3.68. If $C_1, \cdots, C_r \subset G$ are the distinct conjugacy classes, we deduce that

$$|G| = \sum_{i=1}^{r} |C_i|$$

and $|C_i| \mid |G| \; \forall i \in \{1, \cdots, r\}$. This is known as the *class equation*.

We can now prove the following.

Theorem 3.69. *If $|G| > 1$ is a power of some prime number p, then $Z(G)$ is nontrivial (i.e., has more than one element).*

Proof. This essentially follows by Remarks 3.57 and 3.68. Note that every conjugacy class has size dividing $|G|$, so it must be a power of p. Therefore, every conjugacy class has size divisible by p or size 1.

Let's group the conjugacy classes into those of size 1 and those of size p; say $C_1, \cdots, C_s$ have size 1, and $C_{s+1}, \cdots, C_r$ have size divisible by p. Notice that by Remark 3.57, s is just the size of $Z(G)$.

We have

$$|G| = \sum_{i=1}^{r} |C_i| = s + \sum_{i=s+1}^{r} |C_i|,$$

so

$$s = |G| - \sum_{i=s+1}^{r} |C_i|.$$

But $p \mid |G|$, and $p \mid |C_i|$ for $i > s$, so $p \mid s$. Thus $s > 1$, and we are done. □

Recall that Lagrange's theorem says that if G is a finite group and H is a subgroup then $|H|$ divides $|G|$. It is not true, in general, that given any divisor of $|G|$ there is a subgroup of that order. We shall see an example of such a group later. There are, however, partial converses to Lagrange's theorem.

Sylow's Theorem. Let $(G, *)$ be a finite group such that p^n divides $|G|$, where p is prime. Then there exists a subgroup of order p^n.

Proof. Assume that $|G| = p^n m$, where $m = p^r u$ with $HCF(p, u) = 1$. Our central strategy is to consider a cleverly chosen group action of G and prove one of the stabilizer subgroups has size p^n. We'll need to heavily exploit the orbit-stabilizer theorem.

Let S be the set of all *subsets* of G of size p^n. An element of S is an unordered n-tuple of distinct elements in G. There is a natural action of G on S by term-by-term composition on the left.

Let $\omega \in S$. If we fix an ordering $\omega = \{\omega_1, \cdots, \omega_{p^n}\} \in S$, then $g(\omega) := \{g * \omega_1, \cdots, g * \omega_{p^n}\}$.

- We first claim that $|Stab(\omega)| \leq p^n$. To see this define the function

$$\begin{aligned} f : Stab(\omega) &\to \omega \\ g &\to g * \omega_1 \end{aligned}$$

  By the cancellation property for groups this is an injective map. Hence $|Stab(\omega)| \leq |\omega| = p^n$.

- Observe that

$$|S| = \binom{p^n m}{p^n} = \frac{p^n m!}{p^n!(p^n m - p^n)!} = \prod_{j=0}^{p^n-1} \frac{p^n m - j}{p^n - j} = m \prod_{j=1}^{p^n-1} \frac{p^n m - j}{p^n - j}.$$

  Observe that if $1 \leq j \leq p^n - 1$ then j is divisible by p at most $n-1$ times. This means that $p^n m - j$ and $p^n - j$ have the same number of p factors, namely the number of p factor of j. This means that

$$\prod_{j=1}^{p^n-1} \frac{p^n m - j}{p^n - j}$$

  has no p factors. Hence $|S| = p^r v$, where $HCF(p, v) = 1$.

  Now recall that S is the disjoint union of the orbits of our action of G on S. Hence there must be an $\omega \in S$ such that $|Orb(\omega)| = p^s t$, where $s \leq r$ and $HCF(p, t) = 1$. By the orbit-stabilizer theorem we know that $|Stab(\omega)| = p^{n+r-s}\frac{u}{t}$. Because $|Stab(\omega)| \in \mathbb{N}$ and u and t are coprime to p, we deduce that $\frac{u}{t} \in \mathbb{N}$. Hence $|Stab(\omega)| \geq p^n$.

For this choice of $\omega \in S$, $Stab(\omega)$ is thus a subgroup of size p^n. □

Historically this is a slight extension of what is called Sylow's First Theorem. There are two more which describe the properties of such subgroups in greater depth.

3.6 Symmetry of Sets with Extra Structure

Let S be a set and $\Sigma(S)$ its permutation group. The permutation group completely ignores the fact that there may be extra structure on S.

As an example, $\mathbb{R}^n$ naturally has the structure of a vector space. The permutation group $\Sigma(\mathbb{R}^n)$ does not take this into account. However within the full permutation group there are linear permutations, namely $GL_n(\mathbb{R})$. These are permutations which preserve the vector space stucture.

Symmetry in Euclidean Space

Definition 3.70. Given $n \in \mathbb{N}$, n-dimensional Euclidean space is the vector space $\mathbb{R}^n$ equipped with the standard inner product (the dot product).

Concretely, if $\boldsymbol{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \boldsymbol{y} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \in \mathbb{R}^n$ then $\langle \boldsymbol{x}, \boldsymbol{y} \rangle := x_1 y_1 + \cdots + x_n y_n$.

Definition 3.71. The distance between $\boldsymbol{x}$ and $\boldsymbol{y}$ in $\mathbb{R}^n$ is

$$d(\boldsymbol{x}, \boldsymbol{y}) := \sqrt{\langle \boldsymbol{x} - \boldsymbol{y}, \boldsymbol{x} - \boldsymbol{y} \rangle}.$$

Definition 3.72. An **isometry** of $\mathbb{R}^n$ is a map of sets $f : \mathbb{R}^n \to \mathbb{R}^n$ (not necessarily linear) such that $\forall \mathbf{x}, \mathbf{y} \in \mathbb{R}^n$, $d(\mathbf{x}, \mathbf{y}) = d(f(\mathbf{x}), f(\mathbf{y}))$. The collection of all isometries of $\mathbb{R}^n$ is denoted by $Isom(\mathbb{R}^n)$.

Remark 3.73.

- The identity function is an isometry and the composition of any two isometries is an isometry.
- We say an isometry, f, fixes the origin if $f(\mathbf{0}) = \mathbf{0}$. It is a fact that f fixes the origin if and only if $f(\boldsymbol{x}) = \boldsymbol{A}\boldsymbol{x}$ for all $\boldsymbol{x} \in \mathbb{R}^n$, where $\boldsymbol{A}$ is an orthogonal matrix.
- We say an isometry, f, is a translation if

$$\begin{aligned} f : \mathbb{R}^n &\longrightarrow \mathbb{R}^n \\ \boldsymbol{x} &\longrightarrow \boldsymbol{x} + \boldsymbol{y}. \end{aligned}$$

  for some $\boldsymbol{y} \in \mathbb{R}^n$.
- Every isometry of $\mathbb{R}^n$ is a composition of an origin fixing isometry and a translation. As a consequence, all isometries are bijective and their inverses are isometries. This means $Isom(\mathbb{R}^n)$ is a subgroup of $\Sigma(\mathbb{R}^n)$.

Let $X \subset \mathbb{R}^n$ be a subset (not necessarily a subspace).

Definition 3.74. We define the symmetry group of X to be the subgroup $Sym(X) \subset Isom(\mathbb{R}^n)$ with the property that $f \in Sym(X)$ if and only if f permutes X.

There is a natural action of $Sym(X)$ on the set X, coming from the fact there is a natural homomorphism $Sym(X) \to \Sigma(X)$. $Sym(X)$ measures how much symmetry X has. The more symmetric X, the larger $Sym(X)$.

The Dihedral Group

Let $m \in \mathbb{N}$ and $X \subset \mathbb{R}^2$ be a regular m-gon centered at the origin. We call the symmetry group of X the dihedral group of rank m, and we denote it by D_m.

First observe that every element of D_m must fix the center of X (the origin). Thus we may view D_m as a subgroup of the group of 2×2 orthogonal matrices. We shall not take this approach here.

Also observe that $f \in D_m$ acts faithfully and transitive on the set of vertices of X. Hence D_m can naturally by identified with a subgroup of Sym_m. Let σ be the rotation by $\dfrac{2\pi}{m}$ clockwise about the origin. All possible rotational symmetries are generated by σ, namely

$$Rot_m = \{e, \sigma, \sigma^2, \cdots, \sigma^{m-1}\} \subset D_m.$$

Hence Rot_m is cyclic of order m.

Given a vertex a, $Stab(a) = \{e, \tau\}$, where τ is the reflection through the straight line containing a and the origin. By the orbit-stabilizer theorem $|D_m| = 2m$, hence $(D_m : Rot_m) = 2$. We deduce that

$$D_m = Rot_m \coprod \tau Rot_m.$$

The left coset τRot_m is precisely the set of reflective symmetries. Hence every element of D_m can be written in the form σ^k (if a rotation) or $\tau\sigma^k$ (if

a reflection). The group structure is completely determined by the following properties

- $ord(\sigma) = m$
- $ord(\tau) = 2$
- $\tau\sigma = \sigma^{-1}\tau$ (consider the action on the vertices)

Observe that the third property implies that D_m is not Abelian. Here is a picture for $n = 3$.

The Cube in $\mathbb{R}^3$

Let $X \subset \mathbb{R}^3$ be a solid cube centered at the origin. Again, elements of $Sym(X)$ must fix the origin, hence, if we wished, we could identify $Sym(X)$ with a subgroup of the group of 3×3 orthogonal matrices.

Again $Sym(X)$ acts faithfully and transitively on the vertices. If $a \in X$ is a vertex, then $Stab(a)$ can naturally be identified with D_3 (see below figure) which has size 6. Hence, by the orbit-stabilizer theorem, $|Sym(X)| = 48$. The same logic applies to $Rot_\square$, the rotational symmetries, although the stabilizer of a now has size 3. This tells us that $|Rot_\square| = 24$.

If $\tau \in Sym(X)$ is the symmetry sending $\boldsymbol{x}$ to $-\boldsymbol{x}$ (this is not a rotation), then again

$$Sym(X) = Rot_{\square} \coprod \tau Rot_{\square}.$$

It can be shown that $\tau\sigma = \sigma\tau$ for all $\sigma \in Rot_{\square}$. Thus it remains to determine the group structure of $Rot_{\square}$.

Color the vertices with four colors, making sure that opposite vertices have the same color (see below figure). Rotational symmetries act on this set of four colors, inducing a homomorphism from $Rot_{\square}$ to Sym_4. Given any two colors, it is possible to transpose them (leaving the others fixed) by a rotation. Because Sym_4 is generated by transpositions, the induced homormorphism $Rot_{\square} \to Sym_4$ must be surjective. However, $|Rot_{\square}| = 24 = 4! = |Sym_4|$. Hence it must be an isomorphism. We deduce that $Rot_{\square}$ is isomorphic to Sym_4.

Interesting Question:

Let $(G, *)$ be an abstract group. When is it true that we can find $X \subset \mathbb{R}^n$, for some $n \in \mathbb{N}$ such that

$$G \cong Sym(X)?$$

Less formally, when can an abstract group be realised in geometry?

3.7 Normal Subgroups and Isomorphism Theorems

In linear algebra the predominant objects we study are the maps between vector spaces, and not the vector spaces themselves. The structure preserving maps between vector spaces are more interesting than the spaces themselves. This a deep observation and it is true far beyond the confines of linear algebra. Philosophically it's saying that an object in isolation is uninteresting; it's how it relates to what's around it that matters. The world of group theory is no different. Here the objects are groups and the maps between them are homomorphisms. Now we'll study homomorphisms between abstract groups in more detail.

Let G and H be two groups. We'll suppress the $*$ notation as it will always be obvious where composition is taking place. Let e_G and e_H be the respective identity elements. Recall that a homomorphism from G to H is a map of sets $f : G \to H$ such that $\forall x, y \in G$, $f(xy) = f(x)f(y)$.

Definition. Given $f : G \to H$ a homomorphism of groups, we define the **kernel** of f to be:

$$\text{Ker}(f) := \{x \in G \mid f(x) = e_H\}$$

We define the **image** of f to be:

$$\text{Im}(f) := \{y \in H \mid \exists x \in G \text{ such that } f(x) = y\}$$

Proposition. Given a homomorphism $f : G \to H$, $\text{Ker}(f) \subseteq G$ and $\text{Im}(f) \subseteq H$ are subgroups.

Proof. First we will show true for Ker(f):

1. $f(e_G) = e_H \Rightarrow e_G \in Ker(f)$.
2. Suppose $x, y \in Ker(f)$. Then $f(xy) = f(x)f(y) = e_H \Rightarrow xy \in Ker(f)$.
3. Given $x \in Ker(f)$, $f(x^{-1}) = e_H^{-1} = e_H \ \Rightarrow x^{-1} \in Ker(f)$.

Now we will show that Im(f) is a subgroup:

1. $f(e_G) = e_H$ so $e_H \in \text{Im}(f)$.
2. $f(xy) = f(x)f(y) \forall x, y \in G$ so Im(f) is closed under composition.
3. Note that $f(x)^{-1} = f(x^{-1}) \Rightarrow y \in Im(f) \Rightarrow y^{-1} \in Im(f)$.

□

Proposition. A homomorphism $f : G \to H$ is injective if and only if $ker(f)$ is trivial.

Proof. f injective $\Rightarrow Ker(f) = \{e_G\}$ trivially. Now assume $ker(f) = \{e_G\}$. Suppose $x, y \in G$ such that $f(x) = f(y)$.

$$\begin{aligned} f(x) = f(y) &\Rightarrow f(x)f(y)^{-1} = e_H \\ &\Rightarrow f(x)f(y^{-1}) = e_H \\ &\Rightarrow f(xy^{-1}) = e_H \\ &\Rightarrow xy^{-1} = e_G \\ &\Rightarrow x = y \end{aligned}$$

Thus f is injective.

□

Recall that for $m \in \mathbb{N}$ the set of left cosets of $m\mathbb{Z}$ in $\mathbb{Z}$, denoted $\mathbb{Z}/m\mathbb{Z}$ naturally inherited the structure of a group from $+$ on $\mathbb{Z}$. It would be reasonable to expect that this was true in the general case, i.e. given G a group and H, a subgroup, the set G/H naturally inherits the structure of a group from G. To make this a bit more precise let's think about what *naturally* means. Let $xH, yH \in G/H$ be two left cosets. Recall that x and y are not necessarily unique. The only obvious way for combining xH and yH would be to form $(xy)H$.

Warning: in general this is not well defined. It will depend on the choice of x and y.

Something very special happens in the case $G = \mathbb{Z}$ and $m\mathbb{Z} = H$.

Some examples of kernels and images are given in Example 3.77, after the statement of the First Isomorphism Theorem.

Fundamental Definition. We call a subgroup $H \subseteq G$ **normal** if, for all $g \in G$, $gHg^{-1} = \{ghg^{-1} \mid g \in G, h \in H\} = H$. We denote normal subgroup by $H \triangleleft G$.

Remark 3.75.

1. Observe that this is **not** saying that given $g \in G$ and $h \in H$, then $ghg^{-1} = h$. It is merely saying that $ghg^{-1} \in H$. See Example 3.78 for a good example of this.
2. A normal subgroup is the union of conjugacy classes of G.
3. If G is Abelian, every subgroup is normal as $ghg^{-1} = h \forall g, h \in G$.
4. For any group G, the whole group G and the trivial group $\{e_G\}$ are both normal as subgroups.
5. Let G=Sym$_3$, $H = \{e, (12)\}$. Then $(13)(12)(13) = (23) \notin H$

   Hence H is **not** normal in Sym$_3$, so in general not all subgroups of a group are normal.
6. The subgroup $H = \{id, (123), (132)\}$ is normal in $G = Sym_3$.

Proposition 3.76. *Let G and H be two groups. Let $f : G \to H$ a homomorphism. Then $Ker(f) \subset G$ is a normal subgroup.*

Proof. Let $h \in Ker(f)$ and $g \in G$. Then $f(ghg^{-1}) = f(g)f(h)f(g^{-1}) = f(g)e_H f(g)^{-1} = e_H \Rightarrow ghg^{-1} \in Ker(f)$. □

In general $Im(f) \subset H$ is **not** normal.

Fundamental Definition. We say a group G is **simple** if its only normal subgroups are $\{e\}$ and G.

Cyclic groups of prime order are trivially simple by Lagrange's theorem. It is in fact true that for $n \geq 5$, Alt_n is simple, although proving this will take us too far afield. As we shall see later simple groups are the core building blocks of groups theory.

The importance of normal subgroups can be seen in the following:

Proposition. Let $H \subseteq G$ be a normal subgroup. Then the binary operation:

$$G/H \times G/H \to G/H$$

$$(xH, yH) \mapsto (xy)H$$

is well defined.

Proof. As usual the problem is that that coset representatives are not unique and thus we could have two representatives giving different maps. Thus our goal is to show:

$$\forall x_1, x_2, y_1, y_2 \in G \text{ such that } x_1H = x_2H \text{ and } y_1H = y_2H, \text{ then}$$
$$(x_1y_1)H = (x_2y_2)H$$

By assumption we know $x_1^{-1}x_2,\ y_1^{-1}y_2 \in H$. Consider

$$u = (x_1y_1)^{-1}(x_2y_2) = y_1^{-1}x_1^{-1}x_2y_2$$

Hence $uy_2^{-1}y_1 = y_1^{-1}(x_1^{-1}x_2)y_1$. Therefore, by the normality of $H, uy_2^{-1}y_1 \in H \Rightarrow u \in H \Rightarrow (x_1y_1)H = (x_2y_2)H$.

□

This shows that if $H \subset G$ normal, G/H can be endowed with a natural binary operation.

Proposition. Proposition Let G be a group; $H \subset G$ a normal subgroup. Then G/H is a group under the above binary operation. We call it the quotient group.

Proof. Simple check of three axioms of being a group.

1. $\forall x, y, z \in G, (xy)z = x(yz) \Rightarrow (xH * yH) * zH \Rightarrow xH * (yH * zH)$.
2. $xH * H = xH = H * xH \Rightarrow H \in G/H$ is the identity.
3. $xH * x^{-1}H = xx^{-1}H = eH = H = x^{-1}xH = x^{-1}H * xH \Rightarrow$ inverses exist.

□

Proposition. The natural map

$$\begin{aligned} \phi : G &\longrightarrow G/H \\ x &\longrightarrow xH \end{aligned}$$

is a homomorphism with $Ker(\phi) = H$.

Proof. Observe that $\forall x, y \in G$, $\phi(xy) = xyH = xHyH = \phi(x)\phi(y) \Rightarrow \phi$ is a homomorphism.

Recall that the identity element in G/H is the coset H. Hence for $x \in Ker(\phi)$ $\Leftrightarrow \phi(x) = xH = H \Leftrightarrow x \in H$. Hence $Ker(\phi) = H$.

Observe that this shows that any normal subgroup can be realised as the kernel of a group homomorphism.

□

The First Isomorphism Theorem

Let G and H be groups, with respective identities e_G and e_H. Let $\phi : G \to H$ be a homomorphism. Recall that $Ker(\phi) \subset G$ is a normal subgroup. Hence we may form the *quotient* group $G/Ker(\phi)$. Let $x, y \in G$ such that they are in the same left coset of $Ker(\phi)$. Recall that $xKer(\phi) = yKer(\phi) \Leftrightarrow x^{-1}y \in Ker(\phi) \Leftrightarrow \phi(x^{-1}y) = e_H \Leftrightarrow \phi(x^{-1})\phi(y) = e_H \Leftrightarrow \phi(x)^{-1}\phi(y) = e_H \Leftrightarrow \phi(x) = \phi(y)$. In summary, $\phi(x) = \phi(y) \Leftrightarrow xKer(\phi) = yKer(\phi)$ Hence ϕ is **constant** on each coset of $Ker(\phi)$.

Hence we get a map of sets :

$$\begin{aligned} \varphi : G/Ker(\phi) &\longrightarrow Im(\phi) \\ xKer(\phi) &\longrightarrow \phi(x) \end{aligned}$$

This is well define precisely because of the above observations.

The First Isomorphism Theorem. Let G and H be two groups. Let $\phi : G \to H$ be a homomorphism, then the induced map

$$\begin{aligned} \varphi : G/Ker(\phi) &\longrightarrow Im(\phi) \\ xKer(\phi) &\longrightarrow \phi(x) \end{aligned}$$

is an isomorphism of groups.

Proof. Firstly we observe that the induced ϕ is by definition of $Im(\phi)$ surjective. Note that given $x, y \in G$, $\varphi(xKer(\phi)) = \varphi(yKer(\phi)) \Leftrightarrow \phi(x) = \phi(y) \Leftrightarrow xKer(\phi) = yKer(\phi)$, hence φ is injective.

It is left for us to show that φ is a homomorphism. Given $x, y \in G$, $\varphi(xKer(\phi)yKer(\phi)) = \varphi(xyKer(\phi)) = \phi(xy) = \phi(x)\phi(y) = \varphi(xKer(\phi))\varphi(yKer(\phi))$.

Therefore $\phi : G/Ker(\phi) \to Im(\phi)$ is a homomorphism, and thus an isomorphism.

Example 3.77. Here's how the First Isomorphism works for every part of Example 3.3:

1. The inclusion map from $(\mathbb{Z}, +)$ into $(\mathbb{Q}, +)$ is a homomorphism. Its kernel is trivial, and its image is isomorphic to $(\mathbb{Z}, +)$, so it just expresses the fact that for any group G, we have $G/\{e_G\}$ is isomorphic to G.

2. The map from $(\mathbb{Z}, +)$ to $(\mathbb{Z}/m\mathbb{Z}, +)$ sending $a \in \mathbb{Z}$ to $[a] \in \mathbb{Z}/m\mathbb{Z}$ is surjective, so its image is $\mathbb{Z}/m\mathbb{Z}$, and its kernel is $m\mathbb{Z}$. This expresses the fact that $\mathbb{Z}/m\mathbb{Z}$ is indeed the quotient of $\mathbb{Z}$ by $m\mathbb{Z}$, as the notation would suggest.

3. For any group G, the identity map from G to itself is an automorphism of G. Like the first example, this is injective, so its kernel is trivial, so the image is isomorphic to the original group G.

4. Complex conjugation is an automorphism of $(\mathbb{C}, +)$. Same comment as in the previous example.

5. The map from $\mathrm{GL}_n(\mathbb{R})$ to $(\mathbb{R} \setminus \{0\}, \times)$ sending a matrix A to its determinant $det(A)$ is a homomorphism. The kernel is the group $\mathrm{SL}_n(\mathbb{R})$ of matrices with determinant 1. The image is all of $\mathbb{R} \setminus \{0\}$, so this tells us that $\mathrm{GL}_2(\mathbb{R})/\mathrm{SL}_2(\mathbb{R})$ is isomorphic to $(\mathbb{R} \setminus \{0\}, \times)$.

6. The exponential function $x \mapsto e^x$ is a homomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R} \setminus \{0\}, \times)$. Its kernel is trivial, but its image is $\mathbb{R}_{>0} = \{x \in \mathbb{R} \mid x > 0\}$, so it gives an isomorphism between $(\mathbb{R}, +)$ and $(\mathbb{R}_{>0}, \times)$.

7. The complex exponential $z \mapsto e^z$ from $(\mathbb{C}, +)$ to $(\mathbb{C} \setminus \{0\}, \times)$ is a homomorphism. In contrast with the real exponential function, it is surjective but not injective, because $e^z = e^{z+2\pi i}$. Its kernel is $2\pi i\mathbb{Z}$, i.e., all complex numbers of the form $\{2\pi in \mid n \in \mathbb{Z}\}$. This tells us that $(\mathbb{C}, +)/2\pi i\mathbb{Z}$ is isomorphic to $(\mathbb{C} \setminus \{0\}, \times)$.

8. The logarithm is a homomorphism from $(\mathbb{R}_{>0}, \times)$ to $(\mathbb{R}, +)$. In fact, it is an isomorphism, so the same comment as in the first example applies.

9. For any group G and any group H, the map sending all elements of G to $e_H \in H$ is a homomorphism. Its kernel is the whole group G, and is image is the trivial group $\{e_H\}$. The First Isomorphism Theorem here expresses the fact that that for any group G, G/G is isomorphic to the trivial group.

Example 3.78. Consider the group $\mathrm{Aff}(1, \mathbb{R})$ of invertible affine maps from the line $\mathbb{R}$ to itself. This may defined as the subset of $\Sigma(\mathbb{R})$ consisting of maps of the form $x \mapsto ax + b$ for $a, b \in \mathbb{R},\ a \neq 0$.

One can also define it as the set $\mathbb{R} \setminus \{0\} \times \mathbb{R}$, with the binary operation $(a, b) * (c, d) = (ac, ad + b)$. Notice that the group is not abelian. When we write $\mathrm{Aff}(1, \mathbb{R})$, we thus mean $\mathbb{R} \setminus \{0\} \times \mathbb{R}$ *with this group operation.*

The map sending $(a, b) \in \mathbb{R} \setminus \{0\} \times \mathbb{R}$ to $a \in \mathbb{R} \setminus \{0\}$ is a surjective homomorphism from $\mathrm{Aff}(1, \mathbb{R})$ to $(\mathbb{R} \setminus \{0\}, \times)$. The kernel is the set of translations in $\mathrm{Aff}(1, \mathbb{R})$, i.e., the set of elements for which $a = 1$. The subgroup of translations is isomorphic to $(\mathbb{R}, +)$.

Let trans_c denote the translation $x \mapsto x + c$. Notice that if $\sigma = (a, b)$, then $\sigma \mathrm{trans}_c \sigma^{-1}$ is NOT equal to trans_c. Rather, it equals trans_{ac}. Despite this, the set of translations is still a normal subgroup of $\mathrm{Aff}(1, \mathbb{R})$.

□

The Third Isomorphism Theorem

Let G be a group and N a normal subgroup. The third isomorphism theorem concerns the connection between certain subgroups of G and subgroups of G/N.

Let H be a subgroup of G containing N. Observe that N is automatically normal in H. Hence we may form the quotient group $H/N = \{hN \mid h \in H\}$. Observe that H/N is naturally a subset of G/N.

Lemma. $H/N \subset G/N$ is a subgroup.

Proof. We need to check the three properties.

1. Recall that $N \in G/N$ is the identity in the quotient group. Observe that $N \subset H \Rightarrow N \in H/N$.
2. Let $x, y \in H$. By definition $xy \in H$. Thus $xNyN = (xy)N \in H/N$.
3. Let $x \in H$. By definition $x^{-1} \in H$. Thus $(xN)^{-1} = x^{-1}N \in H/N$.

□

Conversely, let $M \subset G/N$ be a subgroup. Let $H_M \subset G$ be the union of the left cosets contained in M .

Lemma. $H_M \subset G$ is a subgroup.

Proof. We need to check the three properties.

1. Recall that $N \in G/N$ is the identity in the quotient group. Hence $N \in M \Rightarrow N \subset H_M$. N is a subgroup hence $e_G \in N \Rightarrow e_G \in H_M$.
2. Let $x, y \in H_M$. This implies that $xN, yN \in M$. M is a subgroup, hence $xNyN = xyN \in M$. This implies that $xy \in H_M$.
3. Let $x \in H_M$. Hence $xN \in M$. M is a subgroup, hence $(xN)^{-1} = x^{-1}N \in M$. This implies that $x^{-1} \in H_M$.

□

Hence we have two maps of sets:

$$\begin{array}{rcl} \alpha : \{\text{Subgroups of } G \text{ containing } N\} & \longrightarrow & \{\text{Subgroups of } G/N\} \\ H & \longrightarrow & H/N \end{array}$$

and

$$\begin{array}{rcl} \beta : \{\text{Subgroups of } G/N\} & \longrightarrow & \{\text{Subgroups of } G \text{ containing } N\} \\ M & \longrightarrow & H_M \end{array}$$

Proposition 3.79. *These maps of sets are inverse to each other.*

Proof. We need to show that composition in both directions gives the identity function.

1. Let H be a subgroup of G containing N. Then $\beta\alpha(H) = \beta(H/N) = H$. Thus $\beta\alpha$ is the identity map on $\{\text{Subgroups of } G \text{ containing } N\}$.
2. Let M be a subgroup of G/N. then $\alpha\beta(M) = \alpha(H_M) = M$. Thus $\alpha\beta$ is the identity map on $\{\text{Subgroups of } G/N\}$.

□

We deduce that both α and β are bijections and we have the following:

The Third Isomorphism Theorem. Let G be a group and $N \subset G$ a normal subgroup. There is a natural bijection between the subgroups of G containing N and subgroups of G/N.

Proof. Either map α or β exhibits the desired bijection. □

Normalizers

Let G be a group and $H \subseteq G$ a subgroup. Given $g \in G$, let

$$gHg^{-1} \coloneqq \{ghg^{-1} \mid h \in H\}.$$

Since conjugation by g is a group automorphism of G, and the image of a subgroup under a homomorphism is also a subgroup, we find that gHg^{-1} is a subgroup of G. Letting $Sub(G)$ denote the set of all subgroups of G, this construction defines an action of G on $Sub(G)$.

The stabilizer of a subgroup H is known as the *normalizer* of H and denoted $N_G(H)$. In other words,

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}.$$

It follows obviously from the definition of normal that H is normal if and only if $N_G(H) = G$.

In fact, more generally, we have that H is a normal subgroup of $N_G(H)$ (but not necessarily of G).

One of your homework problems asks you to commute a normalizer in a simple case.

3.8 Direct Products and Direct Sums

Definition 3.80. Let G and H be two groups, with respective identities e_G and e_H. We may form the **direct product** $G \times H = \{(x, g) \mid x \in G\ g \in H\}$. Let $x, y \in G$ and $g, h \in H$. Observe that there is a natural binary operation on $G \times H$ given by:

$$(x, g) * (y, h) := (xy, gh).$$

Lemma. $G \times H$ is a group under the natural binary operation.

Proof.
1. Associativity holds for both G and $H \Rightarrow$ associativity hold for $G \times H$.
2. (e_G, e_H) is the identity.
3. For $g \in G$ and $h \in H$ $(g, h)^{-1} = (g^{-1}, h^{-1})$.

□

There is an obvious generalization of this concept to any finite collection of groups.

Remark 3.81. The set $\{(x, e_G) \mid x \in G\}$ is a subgroup of $G \times H$ isomorphic to G. It is in fact a normal subgroup, and the quotient by this subgroup is isomorphic to H.

Similarly, there's a subgroup isomorphic to H, and the quotient by this subgroup is isomorphic to G.

Definition 3.82. Let G be a group and $H, K \subset G$ two subgroups. Let us furthermore assume that

1. $\forall h \in H$ and $\forall k \in K$, $hk = kh$.
2. Given $g \in G$ there exist unique $h \in H$, $k \in K$ such that $g = hk$.

Under these circumstances we say that G is the **direct sum** of H and K and we write $G = H \oplus K$. Observe that the second property is equivalent to:

3. $H \cap K = \{e_G\}$ and for $g \in G$ there exist $h \in H$, $k \in K$ such that $g = hk$.

For example, $(\mathbb{Z}/15\mathbb{Z}, +)$ is the direct sum of $gp([3])$ and $gp([5])$.

Proposition 3.83. *If G is the direct sum of the subgroups $H, K \subset G$ then $G \cong H \times K$.*

Proof. Define the map

$$\begin{aligned} \phi : H \times K &\longrightarrow G \\ (h, k) &\longrightarrow hk \end{aligned}$$

Let $x, y \in H$ and $g, h \in K$. By property one $\phi((x, g)(y, h)) = \phi(xy, gh) = xygh = xgyh = \phi(x, g)\phi(y, h)$. Hence ϕ is a homomorphism. Property two ensures that ϕ is bijective. □

Remark 3.84. As in Remark 3.81, the subgroups H and K are normal in G. Then G/K is isomorphic to H, and G/H is isomorphic to K.

The concept of direct sum has a clear generalization to any finite collection of subsets of G.

Note that for us, the main use of the term 'direct sum' is as a way to recognize when a group is the direct product of two of its subgroups. So

3.9 Finitely Generated Abelian Groups

Let G be an Abelian group. We shall now use additive notation to express composition within G. In particular we will denote the identity by 0 (not to be confused with $0 \in \mathbb{Z}$). We do this because we are very familiar with addition on $\mathbb{Z}$ being commutative. Given $m \in \mathbb{Z}$ and $a \in G$, we write

$$ma = \begin{cases} a * a * \cdots * a \ \ (m \text{ times}), & \text{if } m > 0 \\ 0, & \text{if } m = 0 \\ a^{-1} * a^{-1} * \cdots * a^{-1} \ \ (-m \text{ times}), & \text{if } m < 0 \end{cases}$$

We have the identities:

1. $m(a + b) = ma + mb$
2. $(m + n)a = ma + na$
3. $(mn)a = m(na)$

$\forall a, b \in G; m, n \in \mathbb{Z}$

Now assume that G is finitely generated. Hence $\exists\{a_1, \cdots, a_n\} \subset G$ such that $gp(\{a_1, \cdots, a_n\}) = G$. In other words, because G is Abelian, every $x \in G$ can be written in the form

$$x = \lambda_1 a_1 + \cdots + \lambda_n a_n \ \ \lambda_i \in \mathbb{Z}.$$

In general such an expression is not unique. For example is G is of order $m \in \mathbb{N}$ then $(m+1)a = a$ for all $a \in G$. This is because $ma = 0$ A reasonable goal would be to find a generating set such that every expression of the above form was unique (after possibly restricting $0 \leq \lambda_1 < ord(a_i)$) for a given $x \in G$. Such a generating set is called a basis for G. Observe that it is not clear that such a basis even exists at present. If $\{a_1, \cdots, a_n\} \subset G$ were a basis then letting $A_i = gp(a_i) \subset G$ we have the direct sum decomposition:

$$G = A_1 \oplus \cdots \oplus A_n.$$

Conversely, if G can be represented as the direct sum of cyclic subgroups then choosing a generator for each gives a basis for G.

Definition 3.85. Let G be an Abelian group. $x \in G$ is **torsion** is it is of finite order. We denote the subgroup of torsion elements by $tG \subset G$, called the torsion subgroup.

Lemma. $tG \subset G$ is a subgroup.

Proof. This critically requires that G be Abelian. It is not true in general.

1. $ord(0) = 1 \Rightarrow 0 \in tG$
2. Let $g, h \in tG \Rightarrow \exists n, m \in \mathbb{N}$ such that $ng = mg = 0 \Rightarrow nm(g+h) = (mng + nmh) = m0 + n0 = 0 \Rightarrow g + h \in tG$.
3. $ng = 0 \Rightarrow -(ng) = n(-g) = 0$. Hence $g \in tG \Rightarrow -g \in tG$.

□

Clearly if G is finite then $tG = G$.

Definition 3.86. If $tG = G$ we say that G is a torsion group. If $tG = \{0\}$ we say that G is torsion free.

Proposition 3.87. *If G is torsion and finitely generated then G is finite.*

Proof. Let $\{a_1, \cdots, a_n\} \subset G$ be a generating set. Each element is of finite order hence every element $x \in G$ can be written in the form

$$x = \lambda_1 a_1 + \cdots + \lambda_n a_n, \quad \lambda_i \in \mathbb{Z},\, 0 \leq \lambda_1 < ord(a_i).$$

This is a finite set. □

Proposition 3.88. *$G/tG$is a torsion free Abelian group.*

Proof. Firstly note that $tG \subset G$ is normal as G is Abelian, hence G/tG is naturally an abelian group. Let $x \in G$. Assume that $x + tG \in G/tG$ is torsion. Hence $\exists n \in \mathbb{N}$ such that $n(x + tG) = nx + tG = tG$. Hence $nx \in tG$ so $\exists m \in \mathbb{N}$ such that $mnx = 0$. Hence $x \in tG \Rightarrow xtG = tG$. □

Definition. An finitely generated Abelian group G is said to be **free Abelian** if there exists a finite generating set $\{a_1, \cdots, a_n\} \subset G$ such that every element of G can be uniquely expressed as

$$\lambda_1 a_1 + \cdots \lambda_n a_n \text{ where } \lambda_i \in \mathbb{Z}.$$

In other words, if we can find a **basis** for G consisting of non-torsion elements.

In this case

$$G = gp(a_1) \oplus \cdots \oplus gp(a_n) \cong \mathbb{Z} \times \mathbb{Z} \cdots \times \mathbb{Z} = \mathbb{Z}^n.$$

Proposition 3.89. *Let G be a finitely generated free abelian group. Any two bases must have the same cardinality.*

Proof. Let $\{a_1, \cdots, a_n\} \subset G$ be a basis. Let $2G := \{2x \mid x \in G\}$. $2G \subseteq G$ is a subgroup. Observe that $2G = \{\lambda_1 a_1 + \cdots \lambda_n a_n \mid \lambda \in 2]z\}$. Hence $(G : 2G) = 2^n$. But the left hand side is defined independently of the basis. The result follows. □

Definition 3.90. Let G be a finitely generated free Abelian group. The **rank** of G is the size of a any basis.

Theorem 3.91. *A finitely generated abelian group is free Abelan $\Leftrightarrow$ it is torsion free.*

Proof. ($\Rightarrow$) is trivial.

($\Leftarrow$)

Assume G is torsion-free, let $\{a_1, \cdots, a_n\} \subset G$ generate G. We will prove the result by induction on n.

Base Case: $n = 1$. $G = gp(a) \cong (\mathbb{Z}, +)$ which is free abelian. Therefore result is true for $n = 1$.

If $\{a_1, \cdots, a_n\} \subset G$ is a basis we have nothing to prove. Suppose that it is not a basis. then we have a non-trivial relation:

$$\lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_n a_n = 0$$

If $\exists d \in \mathbb{Z}$ such that $d \mid \lambda_i$ for all i, then have $d(\frac{\lambda_1 a_1}{d} + \frac{\lambda_2 a_2}{d} + \cdots + ...) = 0$. As G is torsion-free, $(\frac{\lambda_1 a_1}{d} + \frac{\lambda_2 a_2}{d} + \cdots + ...) = 0$. We can therefore assume that the λ_i are collectively coprime. If $\lambda_1 = 1$, then we can shift terms to get $a_1 = -(\lambda_2 a_2 + \lambda_3 a_3 + \cdots + \lambda_n a_n)$. Therefore, G is generated by the $\{a_2, \cdots, a_n\} \subset G$ and the result follows by induction. We will reduce to this cases as follows: Assume $|\lambda_1| \geq |\lambda_2| > 0$. By the remainder theorem we may choose $\alpha \in \mathbb{Z}$ such that $|\lambda_1 - \alpha\lambda_2| < |\lambda_2|$. Let $a_2' = a_2 + \alpha a_1$ and $\lambda_1' = \lambda_1 - \alpha\lambda_2$, then

$$\lambda_1' a_1 + \lambda_2 a_2' + \cdots + \lambda_n a_n = 0.$$

Also observe that $\{a_1, a_2', \cdots, a_n\} \subset G$ is still a generating set and $\{\lambda_1', \cdots, \lambda_n\}$ are still collectively coprime. This process must must eventually terminate with one of the coefficients equal either 1 or -1. In this case we can apply the inductive step as above to conclude that G is free abelian. $\square$

Proposition 3.92. *Let G be finitely generated and Abelian. Then G/tG is a finitely generated free Abelian group.*

Proof. G/tG is torsion free. We must show that G/tG is finitely generated. Let $\{a_1, \cdots, a_n\} \subset G$ generate G. Then $\{a_1 + tG, \cdots, a_n + tG\} \subset G/tG$ forms a generating set. By the above theorem G/tG is free Abelian. $\square$

Definition 3.93. Let G be a finitely generated Abelian group. We define the rank of G to be the rank of G/tG.

Let G be finitely generated and Abelian. Let G/tG be of rank $n \in \mathbb{N}$ and let $f_1, \cdots, f_n$ be a basis for G/tG. Let $\phi : G \to G/tG$ be the natural quotient homomorphism. Clearly ϕ is surjective. Choose $\{e_1, \cdots, e_n\} \subset G$ such that $\phi(e_i) = f_i \; \forall i \in \{1, \cdots, n\}$. None of the f_i have finite order $\Rightarrow$ none of the e_i have finite order. Moreover

$$\phi(\lambda_1 e_1 + \cdots + \lambda_n e_n) = \lambda_1 f_1 + \cdots + \lambda_n f_n \in G/tG.$$

Because $\{f_1, \cdots, f_n\}$ is a free basis for G/tG we deduce that $\lambda_1 e_1 + \cdots + \lambda_n e_n = 0 \Leftrightarrow \lambda_i = 0 \forall i \Rightarrow F := gp\{e_1, \cdots, e_n\} \subseteq G$ is free abelian with basis $\{e_1, \cdots, e_n\} \Rightarrow F$ is torsion free. Therefore $F \cap tG = \{0\}$.

Let $g \in G$. By definition, $\exists \lambda_1, \cdots, \lambda_n \in \mathbb{Z}$ such that $\phi(g) = \lambda_1 f_1 + \cdots + \lambda_n f_n$. Then we have:

$$\begin{aligned} \phi(g) = \lambda_1 f_1 + \cdots + \lambda_n f_n \quad &\Rightarrow \quad \phi(g) = \phi(\lambda_1 e_1 + \cdots + \lambda_n e_n) \\ &\Rightarrow \quad \phi(g - (\lambda_1 e_1 + \cdots + \lambda_n e_n)) = 0 \\ &\Rightarrow \quad g - (\lambda_1 e_1 + \cdots + \lambda_n e_n) \in ker\phi = tG \\ &\Rightarrow \quad \exists h \in tG \; s.t. \; g = (\lambda_1 e_1 + \cdots + \lambda_n e_n) + h \end{aligned}$$

Hence every x may be written uniquely in the form $x = f + g$ where $f \in F$ and $g \in tG$.

Proposition. Every finitely generated Abelian group can be written as a direct sum of a free Abelian group and a finite group.

Proof. By the above, we may write

$$G = F \oplus tG$$

Define the homomorphism :

$$\begin{aligned} G = F \oplus tG &\longrightarrow tG \\ f + h &\longrightarrow h \end{aligned}$$

This is surjective with kernel F, hence by the first isomorphism theorem tG is isomorphic to G/F. The image of any generating set of G is a generating set for G/F under the quotient homomorphism. Hence tG is finitely generated and torsion, hence finite. F is free Abelian by construction.

□

Hence we have reduced the study of finitely generated Abelian groups to understanding finite Abelian groups.

3.10 Finite Abelian Groups

Definition. A finite group G (not necessarily Abelian) is a **p-group**, with $p \in \mathbb{N}$ a prime, if every element of G has order a power of p.

By Sylow's Theorem the order of a finite p-group must be a power of p. From now on let G be a finite Abelian group. Let $p \in \mathbb{N}$ be a prime. We define $G_p := \{g \in G \mid ord(p) \text{ is a power of } p\} \subset G$.

Theorem 3.94. *$G_p \subset G$ is a subgroup.*

Proof.
1. $ord(0) = 1 = p^0 \Rightarrow 0 \in G_p$.
2. Let $g, h \in G_p \Rightarrow \exists r, s \in \mathbb{N}$ such that $p^r g = p^s h = 0 \Rightarrow p^{r+s}(g + h) = p^s(p^r g) + p^r(p^s h) = 0 + 0 = 0 \Rightarrow g + h \in G_p$.

3. Let $g \in G_p \Rightarrow \exists r \in \mathbb{N}$ such that $p^r g = 0 \Rightarrow -p^r g = p^r(-g) = 0 \Rightarrow -g \in G_p$

□

This critically relies on G being Abelian. By definition G_p is a p-group. Recall that $\forall g \in G$, $\text{ord}(g) \mid |G|$ by Lagrange's Theorem. Therefore $G_p = 0$ unless **possibly** if p divides $|G|$. By Sylow's Theorem we deduce that if $|G| = p^n u$, where $HCF(p, u) = 1$, then $|G_p| = p^n$. Thus $G_p \subseteq G$ is the maximal p-subgroup contained in G. The importance of the maximal p-subgroups is the following theorem.

Theorem 3.95. *Let G is a finite Abelian group. Let $\{p_1, \cdots, p_r\}$ be the primes dividing $|G|$. Then*

$$G = G_{p_1} \oplus \cdots \oplus G_{p_r}$$

Moreover this is the unique way to express as the direct sum of p-subgroups for distinct primes.

Proof. Let $|G| = n = a_1 a_2 \cdots a_r$ where $a_i = p_i^{\alpha_i}$. Let $P_i = n/a_i$. $\{P_1, \cdots, P_r\} \subset \mathbb{Z}$ are collectively coprime $\Rightarrow$ $\exists\ Q_1, \cdots, Q_r \in \mathbb{Z}$ such that

$$P_1 Q_1 + \cdots + P_r Q_r = 1 \text{ (Extension of Euclid)}$$

Let $g \in G$ and $g_i = P_i Q_i g$. Clearly $g = g_1 + g_2 + \cdots + g_r$ and $p_i^{\alpha_i} g_i = Q_i(ng) = 0$. Hence $g_i \in G_{p_i}$.

We must prove the uniquness of this sum. Assume we had

$$g = g_1' + \cdots + g_r', \quad g_i' \in G_{p_i}.$$

Therefore $x = g_1 - g_1' = (g_2' - g_2) + (g_3' - g_3) + \cdots + (g_r' - g_r)$. The right hand size has order dividing P_1, the left hand side has order dividing Q_1. P_1 and Q_1 are coprime $\Rightarrow$ $\exists\ u, v \in \mathbb{Z}$ such that $up_1 + vq_1 = 1 \Rightarrow x =$

$u(p_1x) + v(q_1x) = 0 + 0 = 0 \Rightarrow g_1 = g_1'$. Similarly we find $g_i = g_i'$ for all $i \in \{1, \cdots, r\}$, hence the sum is unique and we deduce

$$G = G_{p_1} \oplus \cdots \oplus G_{p_r}.$$

Let $\{q_i, \cdots, q_s\}$ be a finite collection of distinct primes. Assume that G can be expressed as the direct sum

$$G = H_1 \oplus \cdots \oplus H_s \cong H_1 \times \cdots \times H_s$$

where H_i is a finite q_i-subgroup. Clearly $G_{q_i} = H_i$ and if p is a prime not in $\{q_1, \cdots, q_s\}$ $G_p = \{0\}$. Thus $\{p_1, \cdots, p_r\} = \{q_1, \cdots, q_s\}$ and any such representation is unique. □

We have however reduced the study of finite abelian groups to finite abelian p-groups.

Theorem 1. Every finite Abelian p-group is a direct sum of **cyclic groups**.

Proof. Let G be a finite Abelian p-group. If G is cyclic, we are done, otherwise take a cyclic subgroup $B = gp(b)$ of maximal order, say p^n. Our strategy is to show that there is a p-subgroup $D \subset G$ such that $G = B \oplus D$. We apply the following inductive hypothesis: For any finite Abelian p-group F of size less than $|G|$, if $M \subset F$ is a maximal cyclic subgroup then there exists $N \subset F$ such that $M \oplus N = F$. This is clearly true for F trivial.

We claim that there is a subgroup C of order p such that $B \cap C = \{0\}$. Recall that because G is Abelian G/B is naturally an Abelian p-group. Let $c \in G \setminus B$ and suppose $cB \in G/B$ has order p^r for $r > 0$. Observe that the maximal order of any element in G/B is less than or equal to p^n. Thus we know $n \geq r$. By definition $p^r(cB) = B \Rightarrow p^r c \in B$. Thus there exists $s \in \mathbb{N}$ such that $p^r c = sb$. By maximality of the order of b we know $0 = p^n c = sp^{n-r}b$. But $ord(b) = p^n$, hence $p^n | sp^{n-r}$. Therefore we have $p|s$, say $s = ps'$. Hence $c_1 = p^{r-1}c - s'b$ has order p and is not in B. Therefore $C = gp(c_1)$ is the required subgroup.

Let $BC = \{ab \mid a \in B, b \in C\}$. We claim that $BC \subset G$ is a subgroup.

1. $e_G \in B$ and $e_G \in C \Rightarrow e_G \in BC$.
2. Let $a_1, a_2 \in B$, $b_1, b_2 \in C$. Then $(a_1b_1)(a_2b_2) = (a_1a_2)(b_1b_2) \in BC$. Hence BC is closed under composition.
3. Let $a_1 \in B$, $b_1 \in C$. Then $(a_1b_1)^{-1} = b_1^{-1}a_1^{-1} = a_1^{-1}b_1^{-1} \in BC$. Hence BC is closed under taking inverses.

First observe that $|G/C| < |G|$. Hence the inductive hypothesis applies to G/C. Observe that $BC \subset G$ is a subgroup containing C. Observe that BC/C is cyclic, generated by $bC \in BC/C$. Because $B \cap C = \{0\}$ we also know that $|BC/C| = p^n$. Note that the size of the maximal cyclic subgroup of G must be larger than or equal to the size of the maximal cyclic subgroup of G/C. However we have constructed a cyclic subgroup $BC/C \subset G/C$ whose order equals that of a B. Hence $BC/C \subset G/C$ is a maximal cyclic subgroup. Thus by our inductive hypothesis $\exists N \subset G/C$ such that $BC/C \oplus N = G/C$. By the third isomorphism theorem we know that $N = D/C$ for a unique subgroup $D \subset G$ containing C. We claim that G is the direct sum of B and D.

Let $g \in G$. Then $gC \in G/C$ is uniquely expressible in form $g + C = (a+C)+(d+C) = (a+d)+C$, where $a \in B$ and $d \in D$. Hence $g = a+d+e$ for some $c \in C$. However $C \subset D$ so this expresses g as a sum of elements of B and D. Let $x \in B \cap D$. Hence $xC \in BC/C \cap D/C$. Assume that $x \neq 0$. Note that $x \notin C$. Hence xC is non-zero on BC/C and D/C. However by construction $BC/C \cap D/C = \{C\}$. This is a contraction. Hence $B \cap D = \{0\}$ and we deduce that $G = B \oplus D$.

Thus we have shown that given any finite Abelian p-group G and a maximal cyclic subgroup $B \subset G$, there exists a subgroup $D \subset G$ such that $G = B \oplus D$. Observe that D is a finite Abelian p-group, thus we can continue this process until eventually it must terminate. The end result will be an expression of G as a direct sum of cyclic p-groups.

□

Corollary 3.96. *For any finite Abelian p-group G , there exist a unique decreasing sequence of natural numbers $\{r_1, \cdots, r_n\} \subset \mathbb{N}$ such that*

$$G \cong \mathbb{Z}/p^{r_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{r_n}\mathbb{Z}.$$

Proof. By the previous theorem we know that G is the direct sum of cyclic groups each of p-power order. Thus we know that such integers exist . We will prove uniqueness by induction on $|G|$. Assume that there is are isomorphisms

$$G \cong \mathbb{Z}/p^{r_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{r_n}\mathbb{Z} \cong \mathbb{Z}/p^{s_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{s_m}\mathbb{Z},$$

where the r_i and s_j are a decreasing sequence of natural numbers. We therefore see that $|G| = p^{\sum_{i=1}^{n} r_i} = p^{\sum_{j=1}^{m} s_j}$. Hence $\sum_{i=1}^{n} r_i = \sum_{j=1}^{m} s_j$.

Let $pG = \{pg \mid g \in G\}$. It is a straightforward exercise (which we leave to the reader) to prove that pG is a subgroup of G. Note that for $r > 1$, $\mathbb{Z}/p^{r-1}\mathbb{Z} \cong p(\mathbb{Z}/p^r\mathbb{Z})$, where the isomorphism is given by sending $a + p^{r-1}\mathbb{Z}$ to $pa + p^r\mathbb{Z}$. We deduce therefore that there are isomorphisms

$$pG \cong \mathbb{Z}/p^{r_1-1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{r_n-1}\mathbb{Z} \cong \mathbb{Z}/p^{s_1-1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{s_m-1}\mathbb{Z}.$$

Observe now that $|pG| < |G|$, thus by induction we deduce that the r_i and s_j agree when restricted to entries strictly greater than 1. This, together with the fact that $\sum_{i=1}^{n} r_i = \sum_{j=1}^{m} s_j$, implies that the two sets are the same and thus uniqueness is proven. □

Proposition 3.97. *Let G is an Abelian group such that $p \in \mathbb{N}$ is a prime dividing $|G|$. Then G_p is non-trivial.*

Proof. Recall that if $\{p_1, \cdots, p_r\}$ are the primes dividing $|G|$ then

$$G \cong G_{p_1} \times \cdots \times G_{p_r}.$$

Hence $|G| = |G_{p_1}| \cdots |G_{p_r}|$. By the above corollary p_i divides $|G|$ if and only if G_{p_i} is non-trivial. □

Structure Theorem for Finitely Generated Abelian Groups. Every finitely generated Abelian group G can be written as a direct sum of cyclic groups:

$$G = \beta_1 \oplus \cdots \oplus \beta_r$$

where each β_i is either infinite or of prime power order, and the orders which occur are uniquely determined (up to reordering of the indices).

Proof. $G{=}F \oplus tG$. F is free and finitely generated, hence the direct sum of infinite cyclic groups $(\mathbb{Z}, +)$. The number equals the rank of G. tG is finite Abelian, hence the is the unique direct sum of p-groups for distinct primes p. Each p-group is the unique direct sum (up to order) of p-power cyclic groups. □

Note that we could have stated this theorem with direct product in place of direct sum. Thus we have classified all finitely generate Abelian groups up to isomorphism.

3.11 The Classification of Finite Groups (Proofs Omitted)

In the last section we classified all finite Abelian groups up to isomorphism. Is it possible to do the same for all finite groups? It turns out that the situation is far more complicated in the non-Abelian case.

Here is the basic strategy:

- Show that any finite group G can be broken down into simple pieces.
- Classify these simple pieces.
- Understand how these simple pieces can fit together.

Definition 3.98. let G be a finite group. A ***composition series*** for G is a nested collection of subgroups

$$\{e\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_{r-1} \triangleleft G_r = G.$$

such that

- $G_{i-1} \neq G_i$ for all $0 < i \leq r$.
- G_i/G_{i-1} is simple for all $0 < i \leq r$.

Remark 3.99. By the third isomorphism theorem a composition series cannot be extended, meaning we cannot add any intermediate normal subgroups.

Theorem 3.100. *Any finite group G has a composition series.*

Observe that if G is simple that $\{e\} = G_0 \triangleleft G_1 = G$ is a composition series.

If $G = Sym_3$ then

$$\{e\} \triangleleft gp((123)) \triangleleft Sym_3$$

gives a composition series. To see why, observe that each quotient group has size 3 or 2 and are therefore isomorphism to $\mathbb{Z}/3\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z}$ which are both.

Jordan-Holder Theorem. Let G be a finite group. Suppose we have two composition series for G

$$\{e\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_{r-1} \triangleleft G_r = G.$$

$$\{e\} = H_0 \lhd H_1 \lhd \cdots \lhd H_{s-1} \lhd H_s = G.$$

Then $r = s$ and the quotient groups

$$\{G_1/G_0, \cdots, G_r/G_{r-1}\}, \quad \{H_1/H_0, \cdots, H_s/H_{s-1}\}$$

are pairwise isomorphic (perhaps after reordering).

Definition 3.101. If G has composition series

$$\{e\} = G_0 \lhd G_1 \lhd \cdots \lhd G_{r-1} \lhd G_r = G.$$

we call the quotient groups

$$\{G_1/G_0, \cdots, G_r/G_{r-1}\}$$

the ***simple components*** of G.

By the Jordan-Holder Theorem the simple components are well-defined up to isomorphism. It is possible that two non-isomorphic groups have the same (up to isomorphism) simple components. As an example Sym_3 and $\mathbb{Z}/6\mathbb{Z}$ both have simple components $\{\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}\}$.

Definition 3.102. A finite group is called solvable (or soluble) if its simple components are Abelian. Note that Solvable groups need not be Abelian themselves

Note thatSym_3 is solvable, while Alt_5 (being simple and non-Abelian) is non-solvable.

To summarize our study: Finite group theory if much like the theory of chemical molecules.

- The simple groups are like atoms
- Finite groups have simple components, like molecules have constituent atoms.
- Non-isomorphic finite groups with the same simple components are like molecules with the same atoms but different structure (isomers).

We now have two goals

- Classify all finite simple groups up to isomorphism.
- Classify all finite simple groups with given simple components.

The theory of groups was initiated by Galois in 1832. Galois was the first to discover the first known simple groups, namely $\mathbb{Z}/p\mathbb{Z}$ for p prime and Alt_n for $n > 4$. Amazingly it took until 2004 until a complete classification was known. The proof stretches across over 10000 pages and is the combined work of thousands of mathematicians. Here's a very rough breakdown the the different four distinct classes of finite simple group:

- Cyclic groups of prime order. These are the only Abelian simple groups.
- Alt_n for $n > 4$
- Finite groups of Lie type. These groups are very complicated to describe in general. The basic idea is that they can be realized as subgroups and quotients of matrix groups. There are 16 infinite families of finite simple groups of Lie type.
- There are 26 sporadic groups. Very strangely these do not fall into any fixed pattern. The first were discovered in 1852 by Mathieu, while he was thinking about subgroups of finite permutation groups with extremely strong transitivity properties. The largest sporadic group was discovered in the 1970s. It's called the monster group and has size

  $$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$$

  The monster contains all but six of the other sporadic groups as quotients of subgroups.

The theory of finite simple groups is one of the crown jewels of mathematics. It's demonstrates how profound the definiton of a group really is. All of this complexity is contained in those three innocent axioms.

The next question, of course, is to classify all finite groups with given simple components. This is still a wide open problem. As such a complete classification of all finite groups is still unknown.

One may ask about classifying infinite groups. Unsurprisingly the situation is even more complicated, although much progress has been made if specific extra structure (topological, analytic or geometric) is imposed.

4 Rings, Ideals, and Homomorphisms

4.1 Basic Definitions

A group $(G, *)$ is a set with a binary operation satisfying three properties. The motivation for the definition reflected the behavior of $(\mathbb{Z}, +)$. Observe that $\mathbb{Z}$ also comes naturally equipped with multiplication $\times$. In the first lectures we collected some of the properties of $(\mathbb{Z}, +, \times)$. Motivated by this we make the following fundamental definition:

Definition. A **ring** is a set R with two binary operations, $+$, called addition, and $\times$, called multiplication, such that:

1. R is an **Abelian group** under addition.
2. R is a **monoid** under multiplication (inverses do not necessarily exist).
3. $+$ and $\times$ are related by the distributive law:
   $(x + y) \times z = x \times z + y \times z$ and $x \times (y + z) = x \times y + x \times z \; \forall x, y, z \in R$

The identity for $+$ is "zero", denoted 0_R (often just written as 0), and the identity for $\times$ is "one", denoted 1_R (often just written as 1).

Remark 4.1.
1. To simplify the notation we will write $x \times y = xy$ for all $x, y \in R$.
2. Distributivity implies that we can "multiply" together finite sums:

$$(\sum x_i)(\sum y_j) = \sum x_i y_j$$

   in a well-defined way.

Here are some examples of rings:

1. The integers under the usual addition and multiplication.

2. The rational numbers under the usual addition and multiplication.

3. The real numbers under the usual addition and multiplication.

4. The complex numbers under the usual addition and multiplication.

5. $\mathbb{Z}/m\mathbb{Z}$ under the addition and multiplication described in 2.3.

6. Let S be a set and $\mathbb{P}(S)$ be the set of all subsets. This is called the power set of S. On $\mathbb{P}(S)$ define $+$ and $\times$ by

$$X + Y = (X \cap Y') \cup (X' \cap Y),\ XY = X \cap Y$$

   Where X' denotes the complement of X in S. Then $\mathbb{P}(S)$ is a ring with $\emptyset = 0$ and $S = 1$. This strange looking ring has applications to mathematical logic.

7. In linear algebra the collection of linear maps from $\mathbb{R}^n$ to $\mathbb{R}^n$ is the set $\mathbb{M}_{n\times n}(\mathbb{R}^n)$ (also denoted $\mathbb{M}_n(\mathbb{R}^n)$). This has the structure of a ring under the usual addition and multiplication of matrices. This is an example of a non-commutative ring.

8. The product ring $\mathbb{Z} \times \mathbb{Z}$. It is defined as the set of pairs of integers, with addition and multiplication defined component-wise.

9. More generally, if $(R, +_R, \times_R)$ and $(S, +_S, \times_S)$ are rings, we define the product ring

$$(R \times S, +_{R\times S}, \times_{R\times S})$$

   by

$$(r_1, s_1) +_{R\times S} (r_2, s_2) \coloneqq (r_1 +_R r_2, s_1 +_S s_2) \tag{2}$$
$$(r_1, s_1) \times_{R\times S} (r_2, s_2) \coloneqq (r_1 \times_R r_2, s_1 \times_S s_2) \tag{3}$$

   This can lead to strange rings, such as $\mathbb{Q} \times \mathbb{Z}/5\mathbb{Z}$.

10. If R is any ring, then the set $M_{n\times n}(R)$ of $n \times n$ matrices with coefficients in R is a ring, with addition component-wise, and multiplication defined by the usual formulas for matrix multiplication. If $n \geq 2$, this is not commutative.

11. If R is any ring, there is a ring $R[x]$ of polynomials in the variable x with coefficients in R. A polynomial is a sequence $a_0+a_1x+a_2x^2+\cdots+a_nx^n$, where $a_i \in R$ for $0 \leq i \leq n$. Addition and multiplication are defined like usual addition and multiplication of polynomials. We discuss this in much more detail in Section 4.4.

12. The subset of $\mathbb{C}$ defined by

$$\{a + bi \mid a, b \in \mathbb{Z}\},$$

with the usual operations of addition and multiplication, is a ring known as the *Gaussian Integers*. This ring is denoted $\mathbb{Z}[i]$.

13. The subset of $\mathbb{R}$ defined by

$$\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

is a ring. This ring is denoted $\mathbb{Q}[\sqrt{2}]$. There is also a version $\mathbb{Z}[\sqrt{2}]$ with integer instead of rational coefficients.

Note that matrix multiplication is not commutative in general. So it is perfectly possible for a multiplication not to be commutative in a ring.

Definition 4.2. Let R be a ring with multiplication $\times$. If $\times$ is commutative, i.e. $xy = yx \ \forall \ x, y \in R$ then we say that R is a **commutative ring**.

Definition 4.3. Let R and S be two rings. A **homomorphism** ϕ from R to S is a map of sets $\phi : R \to S$ such that $\forall x, y \in R$

1. $\phi(x + y) = \phi(x) + \phi(y)$
2. $\phi(xy) = \phi(x)\phi(y)$
3. $\phi(1_R) = 1_S$

Once again, if $R = S$ and $\phi = Id_R$ then we call it the identity homomorphism.

Note that R and S are abelian groups under $+$ so ϕ is a group homomorphism with respect to $+$ so $\phi(0_R) = 0_S$. We have to include (3) as $(R, \times)$ is only a monoid, so it does not follow from (2) alone that $\phi(1_R) = 1_S$.

Remark 4.4.

Example 4.5. Here's an example that shows why the last remark is important. The map from $\mathbb{Z}$ to $\mathbb{Z} \times \mathbb{Z}$ sending $n \in \mathbb{Z}$ to $(n, 0) \in \mathbb{Z} \times \mathbb{Z}$ satisfies the first two properties of ring homomorphisms, but it is NOT a ring homomorphism. That's because the multiplicative identity of $\mathbb{Z} \times \mathbb{Z}$ is $(1, 1)$.

1. As for groups, the composition of two ring homomorphisms is again a ring homomorphism.
2. As before, an **isomorphism** is a bijective homomorphism, or equivalently one with an inverse homomorphism. A homomorphism from R to itself is called an **endomorphism**. An endomorphism which is also an isomorphism is called an **automorphism**. This is exactly the same terminology as for groups.

Example 4.6. Here are some examples of ring homomorphisms:

1. The inclusion map from $\mathbb{Z}$ into $\mathbb{Q}$ is a ring homomorphism.
2. More generally, the inclusion map from $\mathbb{Q}$ into $\mathbb{R}$, the inclusion map from $\mathbb{R}$ into $\mathbb{C}$, and the compositions of any of the above are ring homomorphisms.
3. The map from $\mathbb{Z}$ to $\mathbb{Z}/m\mathbb{Z}$ sending $k \in \mathbb{Z}$ to $[k] = k + m\mathbb{Z} \in \mathbb{Z}/m\mathbb{Z}$ is a ring homomorphism. This known as the *projection* or *reduction* homomorphism.
4. The identity map from a ring to itself is always a ring homomorphism (in fact an isomorphism).
5. Complex conjugation, the map from $\mathbb{C}$ to $\mathbb{C}$ sending $a + bi$ to $a - bi$, is a ring homomorphism. In fact, it is an isomorphism that is not the identity (aka, a *non-trivial automorphism*). Non-trivial automorphisms are very important in Galois theory.
6. There is a ring homomorphism from $\mathbb{R}$ to $M_3(\mathbb{R})$ sending $x \in \mathbb{R}$ to $\begin{pmatrix} x & 0 & 0 \\ 0 & x & 0 \\ 0 & 0 & x \end{pmatrix}$. More generally, we have such a ring homomorphism to $M_n(\mathbb{R})$ for any n.

7. The previous example actually works with $\mathbb{R}$ replaced by ANY ring R (yes, even a finite ring like $\mathbb{Z}/m\mathbb{Z}$).

8. For any ring R and $r \in R$, there is a homomorphism

$$\mathrm{ev}_r \colon R[x] \to R$$

sending $f(x) \in R[x]$ to $f(r) \in R$.

9. There is a homomorphism $\mathrm{ev}_i \colon \mathbb{R}[x] \to \mathbb{C}$ sending a polynomial $f(x) \in \mathbb{R}[x]$ to $f(i) \in \mathbb{C}$. Notice that this homomorphism sends $x^2 + 1$ to 0.

10. There is a homomorphism $\mathrm{ev}_{\sqrt{2}} \colon \mathbb{Q}[x] \to \mathbb{R}$ sending $f(x) \in \mathbb{Q}[x]$ to $f(\sqrt{2}) \in \mathbb{R}$. Its image is $\mathbb{Q}[\sqrt{2}]$. Notice that it sends $x^2 - 2$ to 0.

11. If R, S are two rings, then there is a ring homomorphism $\mathrm{pr}_R \colon R \times S \to R$ sending $(r, s) \in R \times S$ to $r \in R$. There is a similar homomorphism $\mathrm{pr}_S \colon R \times S \to S$ sending (r, s) to $s \in S$. These are called *projection homomorphisms*.

In any ring R we have the following elementary consequences of the axioms:

$$x0 = x(0 + 0) = x0 + x0 \Rightarrow x0 = 0$$

Similarly, $0x = 0$ for all $x \in R$.

If R consists of one element, then $1 = 0$, conversely if $1 = 0$ then $\forall x \in R, x = x1 = x0 = 0$, hence R consists of one element. The ring with one element is called the **trivial ring**.

In a ring we abbreviate expressions like

$$a + a + a + \cdots + a \ (n \ times) = na (n \in \mathbb{N})$$

It is clear that we may naturally extend this to all $n \in \mathbb{Z}$.

Similarly,

$$a \times a \times \cdots \times a \ (n \ times) = a^n \ for \ n \in \mathbb{N}.$$

By the Distributive Law, we have the identities

1. $m(a+b) = ma + mb$
2. $(m+n)a = ma + na$
3. $(mn)a = m(na)$

$\forall a, b \in R$ and $m, n \in \mathbb{Z}$.

Definition 4.7. Given R and S two rings we say that R is a **subring** of S if it is a subset and is a ring under the induced operations (with same 0 and 1). Eg. $(\mathbb{Z}, +, \times) \subset (\mathbb{Q}, +, \times)$. More precisely,

1. R is a subgroup of S under addition.
2. R is closed under multiplication.
3. $1_S \in R$.

Remark 4.8. As with subgroups, an arbitrary intersection of subrings is again a subring.

4.2 Ideals, Quotient Rings and the First Isomorphism Theorem for Rings

Let G and H be groups and $\phi : G \to H$ a group homomorphism. Recall that $ker(\phi) \subset G$ is a normal subgroup, thus the set of right cosets $G/ker(\phi)$ naturally forms a group (the quotient group). Recall that all normal subgroups arise in this manner. The 1^{st} Isomorphism theorem states that there is a natural isomorphism

$$G/ker(\phi) \cong Im(\phi).$$

Does something analogous hold for rings?

Let R and S be two rings. Let $\phi : R \to S$ be a ring homomorphism.

Definition 4.9. The kernel of ϕ is the subset

$$ker(\phi) := \{r \in R \mid \phi(r) = 0_S\} \subset R.$$

The image of ϕ is the subset

$$Im(\phi) := \{s \in S \mid \exists r \in R \; s.t. \; \phi(r) = s\} \subset S.$$

Remember that ϕ is a group homomorphism with respect to the additive Abelian group structures on R and S. With respect to this structure these definitions are exactly the same as in group theory. In particular we know that

$$ker(\phi) = \{0_R\} \Leftrightarrow \phi \text{ is injective .}$$

We also know that $ker(\phi) \subset R$ and $Im(\phi) \subset S$ are subgroups under addition.

Proposition 4.10. *$Im(\phi) \subset S$ is a subring.*

Proof. We need to check that $Im(\phi)$ is closed under multiplication and contains 1_S. Let $s_1, s_2 \in Im(\phi)$. Hence $\exists r_1, r_2 \in R$ such that $\phi(r_1) = s_1$ and $\phi(r_2) = s_2$. But $s_1 s_2 = \phi(r_1)\phi(r_2) = \phi(r_1 r_2)$. Hence $s_1 s_2 \in Im(\phi)$. Hence $Im(\phi)$ is closed under multiplication.

By definition $\phi(1_R) = 1_S$. Hence $1_S \in Im(\phi)$. Thus $Im(\phi)$ is a subring.

□

If S is non trivial then because $\phi(1_R) = 1_S$ we know that $1_R \notin ker(\phi)$. Hence in this case ker$(\phi) \subset R$ is not a subring. What properties does it satisfy?

1. $ker(\phi) \subset R$ is a subgroup under $+$.

2. Let $a \in ker(\phi)$ and $r \in R$. Observe that $\phi(ra) = \phi(r)\phi(a) = \phi(r)0_S = 0_S$. Hence $ra \in ker(\phi)$. Similarly $ar \in ker(\phi)$. Hence $ker(\phi)$ is closed under both left and right multiplication by **all** of R.

Definition 4.11. Let R be a ring. An ideal $I \subset R$ is a subset which is a subgroup under addition and is closed under both left and right multiplication by all of R. More precisely, if $x \in I$ then $xr, rx \in I$ for all $r \in R$.

Example 4.12. If R is a commutative ring, and $a \in R$, then the set $aR \coloneqq \{ra \mid r \in R\}$ of all *multiples of a in R* is an ideal. Many of our ideals will be of this form.

Remark 4.13. Notice that $\mathbb{Z} \subseteq \mathbb{Q}$ is a subring, but it is NOT an ideal. In particular, the quotient $\mathbb{Q}/\mathbb{Z}$ is a group under addition, but it is NOT a ring, because multiplication is not well-defined. (For example, $1/2$ and $3/2$ represent the same element of $\mathbb{Q}/\mathbb{Z}$, but $\left(\frac{1}{2}\right)^2 = \frac{1}{4}$ and $\left(\frac{1}{2}\right)\left(\frac{3}{2}\right) = \frac{3}{4}$ do not represent the same element of $\mathbb{Q}/\mathbb{Z}$.

We have just shown that the kernel of a homomorphism is always an ideal. An ideal is the ring theoretic analogue of normal subgroup in group theory.

Let $I \subset R$ be an ideal. Recall that $(R, +)$ is an abelian group, Hence $(I, +) \subset (R, +)$ is a normal subgroup. Hence the right cosets R/I naturally have a group structure under addition. We have completely ignored the multiplicative structure on R. Let us define a multiplication by:

$$(a + I) \times (b + I) := (ab) + I, \quad \forall a, b \in R.$$

Lemma. This binary operation is well defined.

Proof. Let $a_1 + I = a_2 + I$ and $b_1 + I = b_2 + I$ where $a_1, a_2, b_1, b_2 \in R$. Observe that

$$a_1b_1 - a_2b_2 = a_1(b_1 - b_2) + (a_1 - a_2)b_2$$

is contained in I because I is an ideal. Thus

$$a_1b_1 + I = a_2b_2 + I.$$

□

Proposition 4.14. *R/I is a ring under the natural operations. We call it the **quotient ring**.*

Proof. This is just a long and tedious exercise to check the axioms which all follow because they hold on R. Unsurprisingly $0 + I$ is the additive identity and $1 + I$ is the multiplicative identity. □

As in the case of groups there is a natural surjective quotient ring homomorphism

$$\phi : R \to R/I.$$

From the definitions we see that $ker(\phi) = I$. We deduce that ideals of a ring are precisely the kernels of ring homomorphisms. This is totally analogous to the group theory situation.

The First Isomorphism Theorem. Let $\phi : R \to S$ be a ring homomorphism. Then the induced map

$$\begin{aligned} \varphi : R/ker(\phi) &\longrightarrow Im(\phi) \\ a + ker(\phi) &\longrightarrow \phi(a) \end{aligned}$$

is a ring isomorphism.

Proof. The first isomorphism theorem for groups tells us that it is an isomorphism of additive group. Hence we merely need to check that it is a ring homomorphism.

Let $a, b \in R$. $\varphi((a + ker(\phi))(b + ker(\phi))) = \varphi(ab + ker(\phi)) = \phi(ab) = \phi(a)\phi(b) = \varphi(a + ker(\phi))\varphi(b + ker(\phi))$. Also $\varphi(1 + I) = \phi(1) = 1$.

Hence φ is a ring homomorphism and we are done.

□

Definition 4.15. An injective ring homomorphims $\phi : R \to S$ is called and **embedding**. By the first isomorphism theorem, R is isomorphic to the subring $Im(\phi) \subset S$.

Example 4.16. Here are some examples of how the First Isomorphism Theorem applies:

1. Most of the examples in Example 4.6 are injective, which means their kernel is the zero ideal $\{0_R\}$ (which is the same as $0_R R$, the set of multiples of 0_R).
2. The kernel of the homomorphism from $\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$ listed in Example 4.6 is $n\mathbb{Z}$, the set of multiples of n.
3. We will later prove that the kernel of $\mathrm{ev}_i \colon \mathbb{R}[x] \to \mathbb{C}$ is $(x^2+1)\mathbb{R}[x]$, the set of multiples of the polynomial x^2+1.
4. As an example of an ideal not of the form aR, consider the ring $R = \mathbb{Z}[x]$, and consider the set of elements of the form

   $$\{5f(x) + xg(x) \mid f(x), g(x) \in \mathbb{Z}\}.$$

   This is the set of polynomials with integers coefficients whose constant term is a multiple of 5. Then the quotient by this ideal is the ring $\mathbb{Z}/5\mathbb{Z}$ (with the usual operations, of course).

   To see this, consider the homomorphism from $\mathbb{Z}[x]$ to $\mathbb{Z}/5\mathbb{Z}$ sending a polynomial $f(x) \in \mathbb{Z}[x]$ to the residue class of its constant term modulo 5. This is a homomorphism because it is the composition of the homomorphism $\mathrm{ev}_0 \colon \mathbb{Z}[x] \to \mathbb{Z}$ with the projection homomorphism $\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$. Its kernel is precisely the ideal mentioned above.

4.3 Properties of Elements of Rings

Definition 4.17. Let R be a ring. An element $a \in R$ is said to be **invertible**, or a **unit**, if it has a multiplicative inverse, i.e. $\exists a' \in R$ such that $a'a = aa' = 1$. We know that such an inverse is unique if it exists, hence we shall write it as a^{-1}. Note that if $1 \neq 0$ then 0 is never invertible. We denote the set of units in R by R^*.

It is clear that for any ring R, $(R^*, \times)$ is a group.

Definition. A non-trivial ring R in which every non-zero element is invertible (i.e $R \setminus \{0\} = R^*$) is called a **division ring** (or **skew field**). If R is a commutative division ring then R is called a **field**.

Remark 4.18.

1. $(\mathbb{Q}, +, \times)$ is the canonical example of a field. Other natural examples include $(\mathbb{R}, +\times)$, $(\mathbb{C}, +, \times)$ and $(\mathbb{Z}/p\mathbb{Z}, +, \times)$, where p is a prime number. There are examples of division rings which are not fields (i.e. not commutative) but we will not encounter them in this course.

2. All of linear algebra (except the issue of eigenvalues existing) can be set up over an arbitrary field. All proofs are exactly the same, we never used anything else about $\mathbb{R}$ or $\mathbb{C}$.

In an arbitrary ring it is possible that two non-zero elements can multiply to give zero. For example, in $\mathbb{M}_{2\times 2}(R)$, the non-zero matrices

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \text{ and } B = \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix}$$

multiply to give the zero matrix.

Definition. Let R be a non-trivial ring. Given $a \in R \setminus \{0\}$, if there exists $b \in R \setminus \{0\}$ such that $ab = 0$ or $ba = 0$, then a is said to be a **zero-divisor**. Note that 0 is not a zero-divsor.

Definition 4.19. A non-trivial ring R with **no zero divisors** is said to be **entire**; a commutative entire ring is called an **integral domain**. More concretely: R is entire if and only if $1 \neq 0$ and $\forall x, y \in R, xy = 0 \Rightarrow x = 0$ or $y = 0$.

$(\mathbb{Z}, +, \times), (\mathbb{Q}, +, \times)$ are integral domains. $(\mathbb{Z}/m, +, \times)$ is an integral domain $\Leftrightarrow m$ prime. The above example shows that $\mathbb{M}_2(\mathbb{R})$ is not entire.

Theorem. A ring R is **entire** $\Leftrightarrow$ its set of non-zero elements forms a **monoid** under multiplication. Another way to state this is that R entire $\Leftrightarrow R \setminus \{0\}$ is closed under multiplication.

Proof. In any ring R observe that if $x, y \in R$ are two non-zero divisors then by definition $xy \in R$ must be a non-zero divisor. Hence, If R is non-trivial the non-zero divisors of R are a monoid under multiplication. If R is entire the set of non-zero divisors is precisely $R\backslash\{0\}$, which implies it is a monoid under multiplication. Conversly if $R\backslash\{0\}$ is a monoid then firstly it is non-empty so R is non-tivial. But if $x, y \in R\backslash\{0\}$ then $xy \in R\backslash\{0\}$. Hence R is entire by definition.

□

Corollary. Any field F is an integral domain.

Proof. If $x, y \in F$, $x \neq 0 \neq y$ then $\exists\ x^{-1}, y^{-1} \in F$ such that $xx^{-1} = x^{-1}x = 1 = yy^{-1} = y^{-1}y$, therefore xy is invertible so is non-zero.

Hence, non-zero elements are closed under multiplication, so F is entire. F is a field so F is commutative, so it is an integral domain. □

Cancellation Law:

Let R be a ring. If $c \in R$ is not a zero-divisor, then for any $a, b \in R$ such that $ca = cb$ or $ac = bc$, then $a = b$.

This is because $ca - cb = c(a - b)$ and $ac - bc = (a - b)c$. In particular, if R is entire, then we can "cancel" any non-zero element. It is important to note that we cannot do this in an arbitrary ring.

Theorem 4.20. *Every **finite** integral domain R is a field.*

Proof. We need to show that $R^* = R \setminus \{0\}$. Let $a \in R \setminus \{0\}$. Define the following map of sets:

$$\psi : R \setminus \{0\} \to R \setminus \{0\}$$

$$r \mapsto ra.$$

ψ is well define because R is an integral domain. By the cancellation law for integral domains, we know thatgiven $r_1, r_2 \in R$ $r_1 a = r_2 a \Rightarrow r_1 = r_2 \Rightarrow \psi$ injective. Since $R\backslash\{0\}$ is finite, ψ is surjective $\Rightarrow \exists\, b \in R\backslash\{0\}$ such that $ba = ab = 1$. Hence a has a multiplicative inverse. Therefore, $R^* = R \setminus \{0\}$. $\square$

4.4 Polynomial Rings

Let R be a ring.

Definition. The **polynomial ring** in x with cofficients in a ring R consists of formal expressions of the form:

$$g(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m, b_i \in R, m \in \mathbb{N}$$

If $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ is another polynomial then we decree that $f(x) = g(x) \Leftrightarrow a_i = b_i\ \forall i$. Note that we set $a_i = 0$ if $i > n$ and $b_j = 0$ if $j > m$. We refer to x as the *indeterminant*, b_m as the *leading coefficient*, and b_0 as the *constant term*.

Addition and multiplication are defined by the rules

1. $f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n$ (if $m \leq n$)
2. $f(x) \times g(x) = (a_0 b_0) + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_2)x^2 + \cdots + a_n b_m x^{n+m}$

We will denote this ring by $R[x]$.

Exercise 4.1. Check this genuinely gives a ring structure on the set of polynomials in x with coefficients in R.

Note that there is a natural embedding:

$$\begin{array}{rcl} \phi : R & \longrightarrow & R[x] \\ a & \longrightarrow & a \text{ (polynomial with } m = 0 \text{ and } a = a_0) \end{array}$$

The image of this embedding is the set of *constant polynomials*.

Remark 4.21.

1. The zero and one elements in $R[x]$ are the image of the zero and one element in R under ϕ.
2. R commutative $\Rightarrow R[x]$ commutative.
3. Given $f(x) \in R[x]$ we can construct a map (of sets):

$$\begin{array}{rcl} \varphi_f : R & \longrightarrow & R \\ a & \mapsto & f(a), \end{array}$$

   where $f(a) \in R$ is the element of R given be replacing x by a. For a general ring R this process can be quite subtle as we shall see.
4. Alternatively, if we fix a and let f vary, we get a ring homomorphism

$$\mathrm{ev}_a \colon R[x] \to R$$

   sending $f(x) \in R[x]$ to $f(a) \in R$.

Definition 4.22. Let R be a ring and $f \in R[x]$ be a non-zero polynomial. We say that $a \in R$ is a **root**, or zero, of f if $f(a) = 0$.

Note that a is a root of f if and only if $x - a$ is in the kernel of ev_a.

Definition 4.23. Let R be a ring and $f \in R[x]$ be a non-zero polynomial. Hence we may write $f = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_0,\ c_i \in R, c_n \neq 0$. We call n the degree of f and write $\deg(f)=n$. If in addition $c_n = 1$, we say that f is *monic*. The elements of degree 0 are precisely the nonzero constant polynomials.

Remark 4.24. If $f(x)$ is the zero polynomial, then its degree is undefined. One may also consider its degree to be $-\infty$ and check that all of the statements in the following theorem still make sense.

Theorem 4.25. *The following facts are true about degree:*

1. $\forall f, g \in R[x] \setminus \{0\}, deg(f+g) \leq max\{deg(f), deg(g)\}$
2. *If* $deg(f+g) \neq max\{deg(f), deg(g)\}$, *then* f *and* g *have the same degree, and their leading coefficients are negatives (additive inverses) of each other.*
3. $\forall f, g \in R[x]\backslash\{0\}$, *if* $deg(f) \neq deg(g)$, *then* $deg(f+g) = max\{deg(f), deg(g)\}$
4. *If* R *is entire, then* $\forall f, g \in R[x]\backslash\{0\} \Rightarrow fg \neq 0$ *and* $deg(fg) = deg(f) + deg(g)$.

Proof. By the definition of degree, (1) and (2) are clear. (3) follows easily from (2). For (4):

Let $deg(f) = n, deg(g) = m$. Then suppose a_n, b_m the leading coefficients of f and g respectively. Hence fg has maximal power of x given by $a_n b_m x^{n+m}$. As R is entire, $a_n b_m \neq 0 \Rightarrow fg \neq 0$ and $deg(fg) = n+m = deg(f)+deg(g)$. □

Corollary. R entire $\Rightarrow R[x]$ entire.

Proof. Immediate from above.

□

Corollary. R an integral domain $\Rightarrow R[x]$ and integral domain.

Proof. Immediate from above.

□

Example 4.26. Note that $R = \mathbb{Z}/15\mathbb{Z}$ is not an entire ring. If we let $f(x) = [1]+[3]x$ and $g(x) = [2]+[5]x$, both in $R[x]$, then $deg(f) = deg(g) = 1$, but

$$deg(fg) = deg([2] + [11]x) = 1 \neq deg(f) + deg(g) = 2.$$

The process of adjoining indeterminants to a ring R can be iterated to form polynomials in more than one variable with coefficients in R. We of course use another symbol for the indeterminants, ie. $R[x][y]$, polynomials in x and y with coefficients in R, e.g. $x^2 + y^2x + x^3y^6$.

We simplify this notation to $R[x][y] = R[x, y]$. Inductively, we define

$$R[x_1, \cdots, x_n] = R[x_1, \cdots, x_{n-1}][x_n]$$

$f \in R[x_1, \cdots, x_n]$ has a unique expression of the form

$$f = \sum a_{i_1 \cdots i_n} x^{i_1} \cdots x_n^{i_n} \ (a_{i_1 \cdots i_n} \in R)$$

where the sum is finite.

Expressions of the form $m_{(i)} = x_1^{i_1} \cdots x_n^{i_n}$ are called **monomials**. The example we'll study most deeply is when R is a field.

Definition 4.27. Similar to the case of one indeterminant, we have evaluation homomorphisms for rings in multiple variables. If $\underline{a} = (a_1, \cdots, a_n) \in R^n$, then we have an evaluation homomorphism

$$\mathrm{ev}_{(a_1, \cdots, a_n)} = \mathrm{ev}_{\underline{a}} \colon R[x_1, \cdots, x_n] \to R$$

defined by sending $f(x_1, \cdots, x_n) \in R[x_1, \cdots, x_n]$ to $f(a_1, \cdots, a_n)$.

Remark 4.28. Notice that $x_i - a_i \in \ker \mathrm{ev}_{\underline{a}}$ for $1 \leq i \leq n$.

4.5 Ring Extensions

let R be a subring of S. Recall that this means R is a subgroup under addition, is closed under multiplication and contains 1_S. In this case, we say that S is a *ring extension* of R.

Given a ring extension S of R and $(a_1, \cdots, a_n) \in S^n$, we have a more general form of evaluation homomorphism:

$$\mathrm{ev}_{(a_1,\cdots,a_n)} = \mathrm{ev}_{\underline{a}} \colon R[x_1, \cdots, x_n] \to S$$

Example 4.29. Let's suppose that $R = \mathbb{Q}$ and $S = \mathbb{R}$, and let $\alpha = \sqrt{2}$. Then we have the evaluation homomorphism

$$\mathrm{ev}_{\sqrt{2}} \colon \mathbb{Q}[x] \to \mathbb{R}$$

The image of this homomorphism is the ring $\mathbb{Q}[\sqrt{2}]$. It follows by the First Isomorphism Theorem (for rings) that $\mathbb{Q}[\sqrt{2}]$ is a quotient of the ring $\mathbb{Q}[x]$ by $\mathrm{ev}_{\sqrt{2}}$. Notice that $x^2 - 2$ is in this ideal; we will explain in Proposition 5.19 and Remark 5.20 why this kernel is precisely the principal ideal $(x^2-2)\mathbb{Q}[x]$.

Remark 4.30. In the preceding example, the kernel of $\mathrm{ev}_{\sqrt{2}}$ contains no nonzero polynomials of degree less than 2, because if it did, then $\sqrt{2}$ would be rational.

However, if we were to take $R = S = \mathbb{R}$ as in Remark 4.21(4), then $\mathrm{ev}_{\sqrt{2}}$ contains the linear polynomial $x - \sqrt{2}$. Therefore, when considering the kernel of an evaluation homomorphism, it's important to specify the domain of the homomorphism (which is not inherent in the notation ev_a).

Definition 4.31. The ring extension of R by $\{\alpha_1, \cdots, \alpha_n\} \subset S$ is the image of $\mathrm{ev}_{(\alpha_1,\cdots,\alpha_n)}$. Equivalently, it is the subring

$$R[\alpha_1, \cdots, \alpha_n] = \{f(\alpha_1, \cdots, \alpha_n) \mid f \in R[x_1, \cdots, x_n]\}$$

This is the intersection of all subrings of S that contain both R and the subset $\{\alpha_1, \cdots, \alpha_n\}$.

4.6 Field of Fractions

What is the process by which we go from $(\mathbb{Z}, +, \times)$ to $(\mathbb{Q}, +, \times)$? Intuitively, we are "dividing" through by all non-zero elements. Let us think more carefully about what is actually happening and try to generalize the construction

to R an integral domain. What is an element of $\mathbb{Q}$? We usually write it in the form $\frac{a}{b}$ with $a, b \in \mathbb{Z}$, $b \neq 0$. This is **not** unique. $\frac{a}{b} = \frac{c}{d} \Leftrightarrow \ ad - bc = 0$.

As we are all aware, we define $+$ and $\times$ by the following rules:

1. $\frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd}$
2. $\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}$

We should therefore think of elements of $\mathbb{Q}$ as pairs of integers (a, b) such that $b \neq 0$, up to an equivalence relation.

$$(a, b) \sim (c, d) \Leftrightarrow ad - cb = 0$$

Hence, $\mathbb{Q}$ can be thought of as $(\mathbb{Z} \times \mathbb{Z} \setminus \{0\}/\sim)$. The well-definedness of $+$ and $\times$ is not obvious and needs checking, i.e. choosing different elements of the same equivalence class should give the same results.

Let us now generalise this construction. Let R be an integral domain. We define the relation on $R \times R \backslash \{0\}$ by:

$$(a, b) \sim (c, d) \Leftrightarrow ad - bc = 0.$$

Proposition. $\sim$ is an equivalence relation.

Proof.

1. $(a, b) \sim (a, b)$ as $ab - ab = 0$ since R is commutative.
2. $(a, b) \sim (c, d) \Rightarrow ad - bc = 0 \Rightarrow bc - ad = 0 \Rightarrow (c, d) \sim (a, b)$
3. Let $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. Then $ad - bc = 0, cf - de = 0$. Consider

$$\begin{aligned} (af - be)d &= adf - bed \\ &= f(ad - bc) + b(cf - de) \\ &= f0 + b0 = 0 \end{aligned}$$

$$d \neq 0 \Rightarrow af - be = 0 \Rightarrow (a, b) \sim (e, f)$$

□

Let us denote the equivalence classes by $(R \times (R \setminus \{0\}))/\sim$. It is convenient to use the usual notation: for $(a, b) \in R \times (R \setminus \{0\})$ we denote the equivalence class containing (a, b) by $\frac{a}{b}$. Let us define multiplication and addition on $R \times R \setminus \{0\}/\sim$ by

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \qquad \frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}$$

Proposition. $+$ and $\times$ are well-defined on $(R \times (R \setminus \{0\}))/\sim$.

Proof. The first thing to note is that if $b, d \in R \setminus \{0\} \Rightarrow bd \in R \setminus \{0\}$ as R is an integral domain. We just need to check that choosing different representatives gives the same answer. It's just an exercise in keeping the notation in order - you can do it. □

Proposition. $0 \in (R \times (R \setminus \{0\}))/\sim$ is given by the equivalence class containing $(0, 1)$. $1 \in R \times (R \setminus \{0\})/\sim$ is given by the equivalence class containing $(1, 1)$.

Proof. For all $(a, b) \in (R \times (R \setminus \{0\}))$,

$$\frac{a}{b} + \frac{0}{1} = \frac{a \times 1 + b \times 0}{b \times 1)} = \frac{a}{b}.$$

$$\frac{a}{b} \times \frac{1}{1} = \frac{a1}{b1} = \frac{a}{b}$$

Both operations are clearly commutative because R is commutative. Hence we are done.

□

It is a straight forward exercise to check that under these operations $(R\times(R\setminus\{0\}))/\sim$ is a commutative ring. Also observe that $(a,b)\in(R\times(R\setminus\{0\}))$ is in the zero class if and only if $a=0$. Similarly (a,b) give the one class if and only in $a=b$. This is good. It's the same as in $\mathbb{Q}$, so we've done something right.

Theorem. $(R\times(R\setminus\{0\}))/\sim$ is a field.

Proof. We just need to check non-zero elements have multiplicative inverses. Let $\frac{a}{b}\in(R\times(R\setminus\{0\}))/\sim$ be non-zero. By the above this implies that $a\neq 0$. Hence $\frac{b}{a}\in(R\times(R\setminus\{0\}))/\sim$. But

$$\frac{a}{b}\times\frac{b}{a}=\frac{ab}{ab}=\frac{1}{1}.$$

Hence we are done. Multiplication:

Let $(a_1,b_1)\sim(a_2,b_2)$ and $(c_1,d_1)\sim(c_2,d_2)$.

□

Definition 4.32. Let R be an integral domain. The *field of fractions* of R is the field $Frac(R):=(R\times(R\setminus\{0\}))/\sim$.

The canonical example is $Frac(\mathbb{Z})=\mathbb{Q}$.

Definition 4.33. Given an integral domain R and indeterminants $\{x_1,\cdots,x_n\}$ we know that $R[x_1,\cdots,x_n]$ is an integral domain. We define

$$R(x_1,\cdots,x_n):=Frac(R[x_1,\cdots,x_n]).$$

Theorem. The map

$$\phi:R\to Frac(R)$$

$$a\mapsto\frac{a}{1}$$

is an embedding.

Proof. We need to check that ϕ is a homomorphism first.

1. Given $a, b \in R$, $\phi(a+b) = \dfrac{a+b}{1} = \dfrac{a}{1} + \dfrac{b}{1} = \phi(a) + \phi(b)$.
2. Given $a, b \in R$, $\phi(ab) = \dfrac{ab}{1} = \dfrac{a}{1} \times \dfrac{b}{1} = \phi(a)\phi(b)$.
3. $\phi(1) = \dfrac{1}{1}$.

To check it is injective we just need to show that the kernel (as a homomorphism of Abelain groups) is trivial.

$\phi(a) = \dfrac{a}{1} = \dfrac{0}{1} \Leftrightarrow a = 0$. Thus the kernel is trivial and so ϕ is injective. □

Corollary 4.34. *Every integral domain may be embedded in a field.*

Proposition. Let R be a field. The natural embedding $R \subset Frac(R)$ is an isomorphism.

Proof. We must show ϕ is surjective. Let ϕ denote the natural embedding $R \subset Frac(R)$. Let $\dfrac{a}{b} \in Frac(R)$. R is a field so there exist b^{-1}, a multiplicative inverse to b. But $\dfrac{a}{b} = \dfrac{ab^{-1}}{1} = \phi(ab^{-1})$. Hence ϕ is surjective. Therefore ϕ is an isomorphism. □

This is backed up by our intuition. Clearly taking fractions of rationals just gives the rationals again.

4.7 Characteristic

4.7.1 Characteristic in a General Ring

For any two rings A, B, we let $\mathrm{Hom}(A, B)$ denote the set of ring homomorphisms from A to B. We then have the following fact:

Fact 4.35. For any ring R, the set $\mathrm{Hom}(\mathbb{Z}, R)$ has *exactly* one element.

This homomorphism from $\mathbb{Z}$ to R sends $0, 1 \in \mathbb{Z}$ to $0_R, 1_R \in R$, and more generally sends $n \in \mathbb{Z}$ to $n_R \in R$.

Definition 4.36. For a ring R, let I denote the kernel of the unique homomorphism $\mathbb{Z} \to R$. Let m denote the unique non-negative positive integer such that $I = m\mathbb{Z}$. Then m is called the *characteristic* of R.

Fact 4.37. By the First Isomorphism Theorem for rings, the image of this homomorphism is a subring of R isomorphic to $\mathbb{Z}/m\mathbb{Z}$ (note that $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$, and $\mathbb{Z}/1\mathbb{Z}$ is the trivial ring).

Example 4.38.

1. Any subring of $\mathbb{C}$ has characteristic 0. This includes $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, etc.
2. A ring has characteristic 1 iff it is the trivial ring.
3. The ring $\mathbb{Z}/m\mathbb{Z}$ has characteristic m. Thus $\mathbb{F}_p \coloneqq \mathbb{Z}/p\mathbb{Z}$ has characteristic p.
4. If R is a ring, then $R[x]$ has the same characteristic as R.
5. More generally, if R is a subring of a ring S, then R and S have the same characteristic.
6. As an example of the previous part, $\mathbb{F}_p[x]$ is a ring of finite characteristic but infinitely many elements.
7. If R_1 has characteristic m_1 and R_2 has characteristic m_2, then the characteristic of $R_1 \times R_2$ is $LCM(m_1, m_2)$.

8. For example, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ has characteristic 4, $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ has characteristic 12, and $\mathbb{Z} \times R$ has characteristic 0 for any R.

In the last example, different elements have different additive orders (i.e., orders as elements of the abelian group $(R, +)$). In an entire ring, however, every element has the same additive order. We therefore now focus our attention on entire rings:

4.7.2 Characteristic in Entire Rings

Let R be entire (non-trivial with no zero-divisors). Recall that $(R, +)$ is an abelian group, hence given $a \in R$ we may talk about its additive order. Recall that if $a \in R$ does not have finite order, then we say it has infinite order.

Theorem. In an entire ring R, the additive order of every non-zero element is the same. In addition, if this order is **finite** then it is **prime**.

Proof. Let $a \in R \setminus \{0\}$ be of finite (additive) order $k > 1$, i.e. k is minimal such that $ka = 0$. This implies $(k \times 1_R)a = 0 \Rightarrow k \times 1_R = 0$ as R is entire and contains no zero-divisors. Therefore if we choose $b \in R \setminus \{0\}$ then $kb = (k \times 1_R)b = 0 \times b = 0 \Rightarrow$ every element has order dividing k. Choosing a with minimal order $k > 1$ ensures that every nonzero element must have order k. If no element has finite order, all elements must have infinite order.

Now assume that $1_R \in R$ has finite order $k > 1$ and that we have factored $k = rs$ in $\mathbb{N}$. Then $k1_R = (rs)1_R = (r1_R)(s1_R) = 0$. Since R entire, either $r1_R = 0$ or $s1_R = 0$. However, since k is the minimal order of 1_R, $r = k$ or $s = k$. Therefore, k must be prime.

□

Fact 4.39. Suppose R an entire ring. R has **characteristic zero** if all of its non-zero elements have infinite additive order, denoted char(R)=0. If all non-zero elements of R are of additive order $p \in \mathbb{N}$, then R is **characteristic p**, or char(R)=p. In this case, R is **finite characteristic**.

When studying abstract fields, the characteristic is very important.

Eg. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all fields (hence entire) of characteristic zero. If p is a prime number $\mathbb{Z}/p\mathbb{Z}$ is a field of characteristic p. We denote this later field by $\mathbb{F}_p$.

Theorem. There is an embedding of $\mathbb{Q}$ in any field F of characteristic 0.

Proof. Let 1_F denote the multiplicative identity in F. Let 0_F denote the additive identity in F. We must find a suitable **embedding** of $\mathbb{Q}$ in F. Because $char(F) = 0$ the natural map homomorphism:

$$\phi : \mathbb{Z} \to F$$

$$n \mapsto n1_F$$

is injective. We claim that it is a homomorphism (of rings). Let $a, b \in \mathbb{Z}$, then $\phi(ab) = ab1_F = ab1_F1_F = a1_Fb1_F = \phi(a)\phi(b)$; $\phi(a+b) = (a+b)1_F = a1_F + b1_F = \phi(a) + \phi(b)$. $\phi(1) = 1_F$. Thus ϕ is an injective homomorphism.

Now we will extend this notion to $\mathbb{Q}$. We define the following map:

$$\psi : \mathbb{Q} \to F$$

$$\frac{n}{m} \mapsto \phi(n)\phi(m)^{-1}$$

We must check that ψ is well defined and is an embedding.

For $a, b, n, m \in \mathbb{Z}$, $\frac{n}{m} = \frac{a}{b} \Rightarrow nb - am = 0$. Therefore

$$\begin{aligned} \phi(nb - am) = \phi(0) = 0_F = \phi(nb) - \phi(am) \quad &\Rightarrow \quad \phi(nb) = \phi(am) \\ &\Rightarrow \quad \phi(n)\phi(b) = \phi(a)(m) \\ &\Rightarrow \quad \phi(n)\phi(m)^{-1} = \phi(a)\phi(b)^{-1} \\ &\Rightarrow \quad \psi(\frac{n}{m}) = \psi(\frac{a}{b}) \end{aligned}$$

This shows that ψ is well defined.

Next: ψ is a homomorphism.

$$\begin{aligned}\psi(\frac{a}{b}+\frac{n}{m}) &= \psi(\frac{am+bn}{bm}) \\ &= (\phi(a)\phi(m)+\phi(b)\phi(n))\phi(bm)^{-1} \\ &= \phi(a)\phi(b)^{-1}+\phi(n)\phi(m)^{-1} \\ &= \psi(\frac{a}{b})+\psi(\frac{n}{m})\end{aligned}$$

$$\begin{aligned}\psi(\frac{a}{b}\frac{n}{m}) &= \psi(\frac{an}{bm}) \\ &= \phi(an)\phi(bm)^{-1} \\ &= \phi(a)\phi(n)\phi(b)^{-1}\phi(m)^{-1} \\ &= \phi(a)\phi(b)^{-1}\phi(n)\phi(m)^{-1} \\ &= \psi(\frac{a}{b})\psi(\frac{n}{m})\end{aligned}$$

By definition $\psi(\frac{1}{1}) = 1_F$. Thus we have a homomorphism. We claim that it is injective.

We must show that the kernel (as a homomorphism of Abelian groups) is trivial. Let $\frac{n}{m} \in \mathbb{Q}$ such that $\psi(\frac{n}{m}) = 0$. Then $\phi(n)\phi(m)^{-1} = 0 \Rightarrow \phi(n) = 0 \Rightarrow n = 0$ as ϕ was already shown to be injective. Therefore the kernel is trivial, so ψ is an embedding. □

Theorem. Let p be a prime number and F a field of characteristic p. There is an embedding of $\mathbb{F}_p$ into F.

Proof. Note that $\{0_F, 1_F, \cdots, (p-1)1_F\} \subseteq F$ is closed under $+$ and $\times$, hence forms a subring. Clearly $\mathbb{F}_p$ is isomorphic to this subring under the embedding

$$\begin{aligned}\psi : \mathbb{F}_p &\longrightarrow F \\ [\mathrm{a}] &\longrightarrow a1_F\end{aligned}$$

□

4.8 Principal, Prime and Maximal Ideals

Definition 4.40. An ideal $I \subset R$ is proper if $I \neq R$.

Note that $I \subset R$ is proper if and only if R/I is a non-trivial ring.

Definition 4.41. Let R be a commutative ring. We say an ideal $I \subset R$ is principal if there exist $a \in R$ such that $I = \{ra \mid r \in R\}$. In this case we write $I = (a)$.

Definition 4.42. Let R be a commutative ring. We say an ideal $I \subset R$ is prime if it is proper and given $a, b \in R$ such that $ab \in I$ then either $a \in I$ or $b \in I$.

Proposition 4.43. *Let R be a commutative ring. Let $I \subset R$ be an ideal. Then I is prime if and only if R/I is an integral domain.*

Proof. I is a proper ideal hence R/I is non-trivial.

Observe that R commutative trivially implies that R/I is commutative. Let $I \subset R$ be prime and assume that R/I has zero divisors. Then there exists $a, b \in R$ such that $a, b \notin I$ but $(a+I)(b+I) = 0+I$. But this trivially implies that $ab \in I$. But this contradicts the fact that I is prime.

Assume that R/I is an integral domain but I is not prime. Hence we can find $a, b \in R$ such that $ab \in I$ but $a, b \notin I$. But then $(a + I)$ and $(b + I)$ are zero divisors, which is a contradiction.

□

Definition 4.44. Let R be a commutative ring. We say that an ideal is maximal if it is maximal among the set of proper ideals. More precisely $I \subset R$ is a maximal ideal if given an ideal $J \subset R$ such that $I \subset J$, then either $I = J$ or $J = R$.

Proposition 4.45. *Let R be a commutative ring. Let $I \subset R$ be an ideal. Then I is maximal if and only if R/I is a field.*

Proof. First observe that R commutative trivially implies that R/I is commutative.

Assume that $I \subset R$ is maximal. Take a non-zero element of R/I, i.e. $a + I$ for $a \notin I$. Consider the ideal $(a) \subset R$. Consider the following new ideal:

$$(a) + I = \{ra + b \mid r \in R, \ \ b \in I\}.$$

Note that this is certainly an ideal because it is closed under addition and scalar multiplication by all R. Note that by construction $I \subset (a) + I$ and $a \in (a)+I$. Hence I is strictly contained in $(a)+I$. But I is maximal. Hence $(a) + I = R$. Thus there exist $r \in R$ and $b \in I$ such that $ra + b = 1$. Hence $(r + I)(a + I) = ra + I = 1 + I$. Thus $(a + I)$ has a multiplicative inverse. Hence R/I is a field.

Assume that R/I is a field. Assume that J is a proper ideal of R which strictly contains I, i.e. I is not maximal. Let $a \in J$ and $a \notin I$. Thus $(a + I)$ is non-zero in R/I. Thus it has a multiplicative inverse. Hence there exists $b \in R$ such that $ab + I = 1 + I$. This implies that $ab - 1 \in I$, which in turn implies that $ab - 1 \in J$. But $a \in J$, hence $1 \in J$, which implies that $J = R$. This is a contradiction. Hence I is maximal. □

Corollary 4.46. *Let R be a commutative ring. Let $I \subset R$ be an ideal. Then I maximal implies that I is prime.*

Proof. I maximal $\Rightarrow$ R/I is a field $\Rightarrow$ R/I is an integral domain $\Rightarrow$ I prime. □

Example 4.47.

1. In $R = \mathbb{Z}$, the ideal $m\mathbb{Z}$ is maximal iff m if a prime number. The only nonmaximal prime ideal is $\{0\}$.
2. In a field, the ideal $\{0\}$ is maximal.

3. In $R = \mathbb{Q}[x]$, the ideal $\{0\}$ is prime but not maximal. The ideals xR, $(x-3)R$, $(x^2+1)R$, (x^2-2), and $(x^2-3)R$, are maximal.

4. In $R = \mathbb{R}[x]$, the ideals $(x^2-2)R$ and $(x^2-3)R$ are not prime, but the ideal $(x^2+1)R$ is maximal (and therefore also prime).

5. In $R = \mathbb{C}[x]$, and $f \in R$, then the ideal fR is maximal iff f is a linear polynomial with nonzero slope.

6. In $R = \mathbb{Z}[x]$, the ideals $\{0\}$, (7), and $(x-3)$ are prime but not maximal, and the ideal $(\{7, x-3\})$ is maximal.

7. If S is an integral domain, and $R = S[x]$, then every ideal of the form $(x-s)R$ is prime, and such an ideal is maximal iff S is a field.

5 Polynomials and Factorization

5.1 Factorisation in Integral Domains

Let R be a ring. In $\mathbb{Z}$ we have the "Fundamental Theorem of Arithmetic" - every non-zero element of $\mathbb{Z}$ is ± 1 times a unique product of prime numbers. Does something analogous hold for R? Clearly, if R is **not** commutative or has zero-divisors the issue is very subtle. Hence we will resrict to the case when R is an integral domain.

At some point, mathematicians proved that the unique factorization theorem holds in some sense in rings such as $\mathbb{Q}[x]$, $\mathbb{F}_p[x]$, and $\mathbb{Z}[i]$ (in fact, it holds in $F[x]$, where F is any field). At some point in the 19th century, they realized, to their dismay, that it does not hold in every integral domain. The most basic example is that of $R = \mathbb{Z}[\sqrt{-5}]$, in which the equality

$$6 = (2)(3) = (1+\sqrt{-5})(1-\sqrt{-5})$$

demonstrates that unique factorization does not hold in R.

In this section, we will define some useful terms to explain what we even *mean* by unique factorization in a general integral domain.

Let $a, b \in R$. As in $\mathbb{Z}$, $a \mid b$ will mean that $\exists\, c \in R$ such that $b = ac$.

5.1.1 Associated Elements

The first thing we have to deal with is what "unique" means in unique factorization. More specifically, in $\mathbb{Z}$, there is the subtlety that a and $-a$ are essentially the same as far as divisibility is concerned. We formalize this with the following notion:

Definition. Two non-zero elements a, b in an integral domain R are *associated* if $a \mid b$ and $b \mid a$, i.e. $\exists\, c, d \in R$ such that $b = ac$ and $a = bd$.

Theorem 5.1. *In R an integral domain, and $a, b \in R$ be two non-zero elements. Then, a and b are associated $\Leftrightarrow$ $a = bu$ for $u \in R^*$.*

Proof. Association of a and $b \Rightarrow a \mid b$ and $b \mid a \Rightarrow \exists c, d \in R$ such that $a = bd$ and $b = ac \Rightarrow a = acd \Rightarrow a = 0$ or $cd = 1$. If $a = 0 \Rightarrow b = 0$, which is not true by assumption. Thus we have $cd = 1 \Rightarrow c, d$ are inverses of each other and thus units. □

Theorem 5.2. *Let R be an integral domain with $a, b \in R$. Then $(a) \subset (b) \Leftrightarrow b \mid a$. Hence a and b are associated if and only if $(a) = (b)$.*

Example 5.3.

1. In $\mathbb{Z}$, m and n are associated if and only if $n = \pm m$.
2. In $\mathbb{Z}[i]$, z and w are associated if and only if z equals $\pm w$ OR $\pm iw$.
3. In $\mathbb{Z}[\sqrt{2}]$, there are infinitely many units, given by all the integer powers of $1 + \sqrt{2}$. Therefore, if $\alpha \in \mathbb{Z}[\sqrt{2}]$, then all elements of the form $\alpha(1 + \sqrt{2})^n$, for $n\mathbb{Z}$, are associated to α. Thus every nonzero element has infinitely many associates.
4. If F is a field, and $R = F[x]$ then the units of R are precisely the polynomials of degree 0 (aka the nonzero constant polynomials). Then $f, g \in R$ are associate iff one is a constant multiple of the other.
5. In general, if S is an integral domain, and $R = S[x]$, then $S^\times = R^\times$. Thus $\mathbb{Z}[x]^\times = \{\pm 1\}$, and two polynomials are associate in $\mathbb{Z}[x]$ iff they are equal or negatives of each other.

6. In $\mathbb{Z}[1/2]$, the units are all numbers of the form $\pm 2^n$ for $n \in \mathbb{Z}$.

7. In $\mathbb{Z}[1/6]$, the units are all numbers of the form $\pm 2^n 3^m$ for $m, n \in \mathbb{Z}$.

5.1.2 Irreducible and Prime Elements

The second issue to address is what does a prime element of R mean? The problem, as we will see, is that we can easily come up with several different natural definitions which are equivalent in $\mathbb{Z}$, but may not be equivalent in every integral domain. Those two notions are those of *prime element* and *irreducible element*, which are equivalent in $\mathbb{Z}$ but not, for example, in $\mathbb{Z}[\sqrt{-5}]$. As we shall see, $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ are all irreducible, but not prime, in $\mathbb{Z}[\sqrt{-5}]$.

Definition 5.4. We call $a \in R \backslash \{0\}$ an **irreducible element** of R if it is a non-unit and is NOT the product of two non-units.

Remark 5.5. Notice that whether an element is irreducible depends on which ring R you're considering. For example, 5 is irreducible in $\mathbb{Z}$, but not irreducible in $\mathbb{Z}[i]$, as $5 = (1+2i)(1-2i)$.

Definition 5.6. An element $a \in R$ is *prime* if the ideal $(a) = aR$ is a prime ideal.

Notice that a is prime if $a \mid bc$ implies $a \mid b$ or $a \mid c$. In particular, Euclid's Lemma states that prime numbers are prime in the sense of Definition 5.6.

Proposition 5.7. *If a is prime in R, then it is irreducible.*

Proof. Suppose that a were reducible, i.e., $a = bc$, where b and c are non-units. Then $a \mid b$ or $a \mid c$, so WLOG let $a \mid b$. Then $b \mid a$, so a and b are associated, hence Theorem 5.1 tells us that $a = bu$ for a unit u. But then $bu = bc$, so since R is an integral domain, we have $c = u$, contradicting the assumption that c is not a unit. □

Example 5.8. 1. In $\mathbb{Z}$, every irreducible element is prime. In fact, this is true in any UFD (definition below).

2. In $\mathbb{Z}[\sqrt{-5}]$, the element 2 is irreducible, but not prime, because it divides $(1+\sqrt{-5})(1-\sqrt{-5})$ yet divides neither $1+\sqrt{-5}$ nor $1-\sqrt{-5}$.

If a is irreducible or prime, then so are all its associates.

In $\mathbb{Z}$, m is irreducible if and only if it is ± 1 times a prime.

5.1.3 Unique Factorization Domains

The Fundamental Theorem of Arithmetic says that every $m \in \mathbb{Z}$ can be factored into irreducible elements in "essentially" one way. Here, essentially means up to switching irreducibles for *associated* irreducibles, i.e. $10 = 2 \times 5 = (-2) \times (-5)$. This motivates the important definition:

Definition. A **unique factorization domain** (UFD) is an integral domain in which every element NOT zero or a unit can be written as the product of **irreducibles**. Moreover, given 2 complete factorizations of the same element

$$x = a_1 \cdots a_n = b_1 \cdots b_m,$$

into irreducibles, $n = m$ and after renumbering a_i is associated to b_i for all $i \in \{1, \cdots, n\}$.

Clearly $\mathbb{Z}$ is a UFD by the Fundamental Theorem of Artithmetic. A natural question to ask is whether all integral domains are UFDs. The answer, rather surprisingly, is no.

Let R be a UFD. Many of the properties of $\mathbb{Z}$ carry over to R. For example we can talk about highest common factor (HCF) and least common multiple (LCM) for two $a, b \in R \setminus \{0\}$.

Definition. Given $a, b \in R \setminus \{0\}$ a highest common factor of a and b is element $d \in R$ such that

1. $d \mid a$ and $d \mid b$

2. Given $d' \in R$ such that $d' \mid a$ and $d' \mid b$, then $d' \mid d$.

Definition. Given $a, b \in R \setminus \{0\}$ a lowest common multiplie of $a, b \in R$ is an element $c \in R$ such that

1. $a \mid c$ and $b \mid c$
2. Given $c' \in R$ such that $a \mid c'$ and $b \mid c'$, then $c \mid c'$.

Remark 5.9.
1. It should be observed that there is no reason to believe that HCFs and LCMs exist in an arbitrary integral domain. Indeed it is not true in general.
2. Clearly a HCF (if it exists) is NOT unique: If d is an HCF of a and b then so is d' for d' associated to d. Similarly for LCM. Hence when we talk about the HCF or LCM of two elements we must understand they are well defined only up to association.

Theorem. In a UFD any two non-zero elements have a HCF. Moreover, if $a = up_1^{\alpha_1} \cdots p_r^{\alpha_r}$ and $b = vp_1^{\beta_1} \cdots p_r^{\beta_r}$ where u, v are units, and the p_i are pairwise non-associated irreducible elements, then $HCF(a, b) = p_1^{\gamma_1} \cdots p_r^{\gamma_r}$ where $\gamma_i = \min(\alpha_i, \beta_i)$.

Proof. Let d be a common factor of a and b. By the uniqueness of complete factorisation we know that (up to association) d is a product of p_i for $i \in \{1, \cdots p_r\}$. Without loss of generality we may therefore assume that $d = \prod_{i=1}^{r} p_i^{\delta_i}$. Again by the uniqueness of complete factorisation d is a common factor of a and $b \Leftrightarrow \delta_i \leq \alpha_i$ and $\delta_i \leq \beta_i \forall i$. Therefore, $\delta_i \leq \gamma_i \Rightarrow HCF(a, b) = p_1^{\gamma_1} \cdots p_r^{\gamma_r}$. □

Proposition. In a UFD any two non-zero elements have a LCM. Moreover, if $a = up_1^{\alpha_1} \cdots p_r^{\alpha_r}$ and $b = vp_1^{\beta_1} \cdots p_r^{\beta_r}$ where u, v are units, and the p_i are pairwise non-associated irreducible elements, then $LCM(a, b) = p_1^{\gamma_1} \cdots p_r^{\gamma_r}$ where $\gamma_i = \max(\alpha_i, \beta_i)$.

Proof. Exactly the same argument as above works in this case observing that $d = \prod_{i=1}^{r} p_i^{\delta_i}$ is a common multiple of a and b if and only if $\delta_i \geq \alpha_i$ and $\delta_i \geq \beta_i$ for all $i \in \{1, \cdots p_r\}$. □

Remark 5.10. If $a \in R$ a unit then

$$HCF(a, b) = 1,\ LCM(a, b) = b\ \forall b \in R \setminus \{0\}$$

5.2 Remainder Theorem for Polynomials

Recall that for a polynomial $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$ where $a_n \neq 0_R$ is said to have degree n. Note that degree is defined only when $f(x)$ is not the zero polynomial. Recall that *if R is an integral domain*, then

$$\deg f(x)g(x) = \deg f(x) + \deg g(x).$$

Note that a polynomial $f(x)$ has degree zero if and only if it is nonzero and constant.

We then have the remainder theorem for polynomials:

Theorem 5.11. *Let F be a field, and let $f(x), g(x) \in F[x]$, with $g(x) \neq 0$ (i.e., it is not the zero polynomial). Then there exist $q(x), r(x) \in F[x]$ such that*

$$f(x) = q(x)g(x) + r(x),$$

where either $r(x) = 0$, or $\deg r(x) < \deg g(x)$.

Proof. Let $f = a_0 + a_1 x + \cdots + a_n x^n$, $g = b_0 + b_1 x + \cdots + b_m x^m$ where $a_i, b_j \in F, n, m \in \mathbb{N} \cup \{0\}$, and $a_n \neq 0, b_m \neq 0$.

Assume $\deg(f) \geq \deg(g) \Rightarrow n \geq m \Rightarrow n - m \geq 0 \Rightarrow x^{n-m} \in F[x] \Rightarrow x^{n-m} b_m^{-1} a_n g$ has leading term $a_n x^n \Rightarrow \deg(f - x^{n-m} b_m^{-1} a_n g) < \deg\,(f)$.

Hence setting $c = a_n b_m^{-1} x^{n-m}$ we have $\deg(f - cg) < deg(f)$. □

Remark 5.12. Notice this proof crucially uses the fact that F is a field, because you might have to divide by a coefficient. Therefore, the theorem is false for $\mathbb{Z}[x]$ in place of $F[x]$, as can be seen by taking $f(x) = x$ and $g(x) = 2$.

Remark 5.13. Notice that this looks very similar to the Remainder Theorem for integers (2.5), with the absolute value in place of the degree function. The notion of *Euclidean Domain* is a generalization of both of these examples, and the absolute value (in the case of $\mathbb{Z}$) and the degree (in the case of $F[x]$) are examples of *Euclidean functions*.

You don't technically need to know the term "Euclidean domain," but you should understand the similarity between the Remainder Theorem for $\mathbb{Z}$ and that for $F[x]$. And that similarity is precisely what the notion of "Euclidean domain" is about.

The Remainder Theorem is useful because it allows one to show that $F[x]$ is a PID, which also implies that it is a UFD. We now talk about PID's.

5.3 PID

Definition 5.14. An integral domain R is a *principal ideal domain (PID)* if every ideal of R is of the form $aR = (a)$ for some element $a \in R$.

Here are a few non-examples:

Example 5.15. The ring $R = F[x, y]$ is not a PID. One may check that the ideal (x, y) is not principal.

Example 5.16. The ring $R = \mathbb{Z}[x, y]$ is not a PID. One may check that the ideal $(2, x)$ is not principal.

Example 5.17. The ring $R = \mathbb{Z}[\sqrt{-5}]$ is not a PID. This is a bit harder, and it follows from 6(b) on HW 11.

Here are some examples:

Example 5.18. The rings $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{-2}]$, and $\mathbb{Z}\left[\frac{\sqrt{-163}+1}{2}\right]$ are PID's. The first four can be proven using methods similar to those used for $F[x]$ below; the last one is harder to prove (and is not something we will cover).

5.3.1 RT implies PID

We now explain how the remainder theorem can be used to show that $F[x]$ is a PID.

Proposition 5.19. *The ring $R = F[x]$ is a PID.*

Proof. Let I be an ideal in R. If $I = \{0\}$ or $I = R$, then I is principal (as it is (0) or (1), respectively).

If not, then I has at least some nonzero element, call it $f(x)$. Then $f(x)$ has a degree, which is a non-negative integer. If $f(x)$ has the smallest possible degree among nonzero elements of I, then we fix $f(x)$; if not, we replace $f(x)$ with an element of I with smallest possible degree (there is always a smallest possible degree, because the degree is ≥ 0). Let this element be $g(x)$.

We want to show that $I = g(x)R$. For this, let $h(x)$ be a general element of I. We want to show that $h(x)$ is a multiple of $g(x)$. For this, apply the remainder theorem to find $h(x) = q(x)g(x) + r(x)$, where $r(x)$ is zero or has smaller degree than $g(x)$. Note that because $g(x), h(x) \in I$, we have $r(x) = h(x) - q(x)g(x) \in I$. Therefore, $r(x)$ cannot have smaller degree than $g(x)$ (by the definition of $g(x)$), so $r(x) = 0$. That means that $h(x) = g(x)q(x)$, so $g(x)$ divides $h(x)$, as desired. □

Remark 5.20. The proof of Proposition 5.19 implies that if I is an ideal and f is an element of I of minimal degree, then f generates I. This is explained in more detail in Proposition 5.30 below.

5.3.2 Consequences of Being a PID

One important fact about PID's is that they are UFD's. We will not give the entire proof of this fact. The proof has two important steps:

1. Showing that factorization into irreducibles exist
2. Showing that that factorization is unique

1. can be proven using the stuff about ascending chains of ideals in 4.10 of Paulin, but we won't worry about that. For 2., an important step is showing that all irreducible elements are prime (this fact is both true in a UFD and is a step in proving that a given ring is a UFD).

Example 5.21. To see why "irreducible implies prime" is related to uniqueness of factorization, consider the ring $\mathbb{Z}[\sqrt{-5}]$, which is neither a PID nor a UFD. Then the fact that $(2)(3) = (1+\sqrt{-5})(1-\sqrt{-5})$ are two different factorizations into irreducibles of the same element (6) is related to the fact that 2 is not prime. Indeed, 2 is irreducible, divides $(1+\sqrt{-5})(1-\sqrt{-5})$, but does not divide either factor. So 2 is *irreducible but not prime.*

Let's now prove that every irreducible element of a UFD is prime. Remember that a nonzero element is prime if and only if the ideal it generates is prime (by definition), and recall that maximal ideals are always prime. Therefore, it suffices to prove that every irreducible element generates an ideal that is maximal:

Proposition 5.22. *Let R be a PID, and suppose $a \in R$ is irreducible. Then aR is maximal.*

Proof. First, note that aR is not R, or else a would be a unit, and by definition irreducible elements are not units.

Now suppose that J is an ideal with $aR \subseteq J \subseteq R$. As R is a PID, we have $J = bR$ for some $b \in R$. Since $a \in aR \subseteq J$, we know that $b \mid a$. As a is irreducible, this means that either b is a unit, or b is associated to a. Int he

former case, we have $J = R$, and in the latter case, we have $J = aR$. As J was arbitrary, this means that aR is maximal. □

As mentioned before, maximal implies prime (for ideals). And in any UFD, every irreducible element is prime. HOWEVER, in UFD's that are NOT PID's, there can be nonzero non-maximal primes. For example:

Example 5.23. In $R = \mathbb{Z}[x]$, let $I = xR$. Then x is in fact prime, but $R/I \cong \mathbb{Z}$, which is an integral domain but not a field. Therefore, I is maximal but not prime. This essentially happens because R is a UFD but not a PID.

In fact, note that the ONLY non-maximal prime ideal in a PID is the zero ideal. Therefore, if R is a PID, then every prime ideal is either aR for $a \in R$ irreducible or $\{0\}$. This latter fact can be used to prove, for example, that $\mathbb{Q}[\sqrt{2}]$ is not just a ring but also a field; for it is the quotient of $\mathbb{Q}[x]$ by the ideal generated by the irreducible polynomial $x^2 - 2$, and this ideal must be maximal.

Here's another fact that holds in PID's but not in general UFD's: Recall that HCF's always exist in a UFD. In a PID, we can say a little bit more about HCF's than just that they exist. Specifically, we can say the following:

Proposition 5.24. *Let R be a PID, $x, y \in R$, and d an HCF of x and y. Then there exist $a, b \in R$ such that $ax + by = d$.*

Proof. Let I be the ideal generated by x and y. Then I is the set of all elements of R of the form $ax + by$ for $a, b \in R$. Thus we have to show that $d \in I$.

Because R is a PID, we know that I is principal, say $I = zR$ for some $z \in R$. Then since $x, y \in I$, we know $z \mid x$ and $z \mid y$. By definition of HCF, we find that $z \mid d$. But then $d \in I = zR$, so we are done. □

5.4 Factorization of Polynomials

We collect some facts about factorization of polynomials that will be useful in our discussion of field extensions in Section 5.5. These facts are mostly just summaries of what was discussed in the previous two sections.

First, here's a description of all the ideals in $F[x]$:

Fact 5.25.

1. Every ideal in $F[x]$ is of the form $(f(x))$ for $f(x) \in F[x]$.
2. Two such ideals $(f(x))$ and $(g(x))$ are the same ideal if and only if $g(x)$ is a nonzero constant multiple of $f(x)$.
3. The only non-maximal prime ideal is (0).
4. The maximal ideals are precisely those of the form $(p(x))$ for an irreducible polynomial $p(x)$.
5. If I is a nonzero ideal, then it has a unique monic generator (recall that monic means the leading coefficient is 1).

Recall that whether a given polynomial is irreducible depends on F. For example, $x^2 - 2$ is irreducible in $\mathbb{Q}[x]$ but not in $\mathbb{R}[x]$.

Now let's talk about how to recognize whether a given element generates an ideal. First, a definition:

Definition 5.26. If I is an ideal in $R = F[x]$, then $f(x)$ has *minimal degree* in I if for any $g(x) \in I \setminus \{0\}$, we have $\deg f(x) \leq \deg g(x)$.

Example 5.27. In $\mathbb{C}[x]$, the ideal generated by $x^3 - x + 1$ has no elements of degrees 0, 1, or 2. All of its elements are either 0 (which does not have a degree) or have degree at least 3.

Example 5.28. More generally, if $f(x)$ is a polynomial of degree n in $F[x]$, then $(f(x))$ has no elements of degree less than n.

Example 5.29. An ideal $I \subseteq F[x]$ has elements of degree zero if and only if it is the whole ring.

We then have the following facts, which essentially follow from the proof of 5.11 and from the facts mentioned above:

Fact 5.30.
1. If I is an ideal of $F[x]$, and if $f(x) \in I$ has minimal degree, then $f(x)$ generates I.
2. Any two elements of I of minimal degree are constant multiples of each other.
3. If I is a nonzero ideal, then I has an element of minimal degree.
4. If I is generated by $0 \neq f(x) \in F[x]$, then $f(x)$ has minimal degree in I.

Finally, we note the following important fact:

Proposition 5.31. *If I is an ideal not equal to R, $p(x) \in I$ is an irreducible element of $F[x]$, then $p(x)$ generates I. In particular, $p(x)$ has minimal degree in I, and any other irreducible $q(x) \in I$ is a nonzero constant multiple of $p(x)$.*

Proof. The ideal $(p(x))$ is then contained in I. Since $(p(x))$ is maximal, and I is not all of R, we must have $I = (p(x))$. □

5.4.1 Linear Factors of Polynomials

Finally, here's an important consequence of the Remainder Theorem. This gives a relationship between factorization of polynomials and roots of polynomials.

Lemma 5.32. *If F is a field, $\alpha \in F$, and $f(x) \in F[x]$, then $(x - \alpha) \mid f(x)$ if and only if $f(\alpha) = 0$.*

Proof. If $(x - \alpha) \mid f(x)$, then $f(x) = (x - \alpha)g(x)$ for some $g(x) \in F[x]$. Therefore, $f(\alpha) = (\alpha - \alpha)g(\alpha) = 0g(\alpha) = 0$.

Conversely, suppose $f(\alpha) = 0$. By the Remainder Theorem, we can write

$$f(x) = q(x)(x - \alpha) + r(x),$$

where $r(x)$ is either zero or has degree 0. Therefore, $r(x)$ is constant. But $r(\alpha) = f(\alpha) - q(\alpha)(\alpha - \alpha) = 0$, so $r(x)$ is just 0. Therefore, $f(x) = q(x)(x - \alpha)$, so $(x - \alpha) \mid f(x)$. □

One can repeatedly apply Lemma 5.32 to show that a polynomial of degree n can have at most n roots.

5.5 Ring and Field Extensions

Recall that if R is a subring of a ring S, and $\alpha \in S$, then there is an evaluation homomorphism

$$\mathrm{ev}_\alpha \colon R[x] \to S,$$

sending $f(x) \in R[x]$ to $f(\alpha) \in S$. The image is a subring of S denoted $R[\alpha]$, and $R[\alpha]$ is the smallest subring of S containing R and α.

If R and S are both fields, then we let $R(\alpha)$ denote the smallest sub*field* of S containing R and α. Note that we always have $R[\alpha] \subseteq R(\alpha)$, and these are equal if and only if $R[\alpha]$ is already a field. We want to understand when this does and doesn't happen.

We now set $F = R$ and $E = S$. The pair of E and F, often denoted E/F, is called a *field extension*. Note that this is NOT any kind of quotient - the use of "/" is just historically a piece of notation used for field extensions.

Given a field extension E/F and $\alpha \in E$, we set

$$I_\alpha \coloneqq \ker \mathrm{ev}_\alpha.$$

Note that I_α is an ideal in $F[x]$, so we can apply everything we know from Section 5.4 to it.

By the first isomorphism theorem for rings, we have $F[\alpha] \cong F[x]/I_\alpha$. Note that E is a field and therefore an integral domain, so it has no zero-divisors. But that means that $F[\alpha]$, being a subring of E, also has no zero-divisors. Therefore, $F[\alpha]$ is an integral domain (ID), so I_α is a prime ideal in $F[x]$.

By Fact 5.25, we either have $I_\alpha = (p(x))$ for $p(x)$ an irreducible element of $F[x]$, or $I_\alpha = \{0\}$. We distinguish these two cases with a pair of definitions:

Definition 5.33. If E/F is a field extension and $\alpha \in E$, then α is *algebraic over* F if I_α has a nonzero element. Equivalently, α is the root of a nonzero polynomial with coefficients in F.

Definition 5.34. If E/F is a field extension and $\alpha \in E$, then α is *transcendental over* F if $I_\alpha = \{0\}$. Equivalently, α is not the root of any nonzero polynomial with coefficients in F.

By Fact 5.25, we find that $F[\alpha]$ is a field (and hence $F[\alpha] = F(\alpha)$) if and only if α is algebraic over F.

Example 5.35. Any element of F itself is trivially algebraic over F.

Example 5.36. The numbers $\sqrt{2}$, $\sqrt{3}$, $\sqrt[3]{2}$, and more generally, $\sqrt[n]{a}$ for $a \in \mathbb{Q}$ and $n \in \mathbb{N}$ are algebraic over $\mathbb{Q}$.

Example 5.37. The complex number i is algebraic over $\mathbb{Q}$ (and over $\mathbb{R}$).

Example 5.38. The numbers $e = 2.71828...$ and $\pi = 3.14159...$ are transcendental over $\mathbb{Q}$. See `https://en.wikipedia.org/wiki/Lindemann%E2%80%93Weierstrass_theorem` for some of the history of this. It was a conjecture of Lambert in 1768, but only proven (in the case of π) in 1882 by Lindemann.

Example 5.39. The number π is algebraic over $\mathbb{R}$, even though it is transcendental over $\mathbb{Q}$. In fact, it is also algebraic over a field like $\mathbb{Q}(\pi^2)$.

The last two examples show that whether an element is transcendental or algebraic depends on the field F. Clasically, people only considered the following definition:

Definition 5.40. A complex number α is said to be *an algebraic number* if it is algebraic over $\mathbb{Q}$. It is said to be *a transcendental number* if it is transcendental over $\mathbb{Q}$.

For some time, people didn't know if there even were transcendental numbers. The first number proven to be transcendental was

$$\sum_{n=1}^{\infty} \frac{1}{10^{n!}},$$

which was done by Liouville. You can find out about more numbers that are known to be transcendental at `https://en.wikipedia.org/wiki/Transcendental_number#Numbers_proven_to_be_transcendental`.

Remark 5.41. This material is non-examinable: The subset of $\mathbb{C}$ consisting of all algebraic numbers is denoted $\overline{\mathbb{Q}}$. It turns out that this subset is in fact a subfield, and it is known as the *algebraic closure of* $\mathbb{Q}$. It is *algebraically closed* in the sense that every polynomial with coefficients in it has a root (and in fact splits into linear factors). You can read more at `https://en.wikipedia.org/wiki/Algebraic_number#The_field_of_algebraic_numbers` and the links contained therein.

5.5.1 Minimal Polynomials

Let E/F be a field extension, and suppose that $\alpha \in E$ is algebraic. Then the ideal $I_\alpha \subseteq F[x]$ has a unique monic generator by Fact 5.25. This generator is called the *minimal polynomial* of α *over* F.

How can we tell if a given polynomial is the minimal polynomial of a given $\alpha \in R$? Well if $p(x) \in F[x]$ is irreducible such that $p(\alpha) = 0$, then Fact 5.31 implies that $p(x)$ generates I_α. Therefore, the unique monic multiple of $p(x)$ is the minimal polynomial of α.

Note that $\alpha \in F$ if and only if its minimal polynomial is $x - \alpha$ (or equivalently, as long as its minimal polynomial is linear).

Example 5.42. The minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $x^2 - 2$.

Example 5.43. The minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}[\sqrt{2}]$ is just $x - \sqrt{2}$.

Example 5.44. The minimal polynomial of i over $\mathbb{Q}$, or even over $\mathbb{R}$, is $x^2 + 1$.

Example 5.45. The minimal polynomial of the Golden Ratio $\dfrac{\sqrt{5}+1}{2}$ over $\mathbb{Q}$ is $x^2 - x - 1$.

In order to find the minimal polynomial of α, it suffices to find a polynomial $f(x) \in F[x]$ such that $f(\alpha) = 0$ and then show that $f(x)$ is irreducible. This latter step can be tricky.

Example 5.46. The minimal polynomial of $\alpha = e^{2\pi i/7} = \cos\dfrac{2\pi}{7} + i\sin\dfrac{2\pi}{7}$ is $f(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$. Note that

$$f(x) = \frac{x^7 - 1}{x - 1},$$

so it is clear that $f(\alpha) = 0$. To show that $f(x)$ is irreducible in $\mathbb{Q}[x]$, one needs to use the Eisenstein Criterion from p.74 of Paulin's notes. However, we will not cover the Eisenstein Criterion in this semester.

We can, however, prove irreducibility in the following cases:

Proposition 5.47. *If $f(x) \in F[x]$ is quadratic or cubic (i.e., degree 2 or 3), then $f(x)$ is irreducible iff $f(x)$ has no root in F.*

Proof. If $f(x)$ were reducible, then because degrees add when you multiply polynomials, it would have to have a (non-constant) linear factor. But any nonconstant linear polynomial over F is of the form $ax + b$ for $a, b \in F$, with $a \neq 0$. Since F is a field, this linear polynomial has a solution $-\dfrac{b}{a} \in F$. Therefore, if $f(x)$ is reducible, then $f(x)$ has a root in F.

Conversely, if $f(x)$ has a root in F, then by Lemma 5.32, it is divisible by a linear polynomial, so it is reducible (since it is quadratic or cubic and therefore not linear). □

Example 5.48. This allows one to prove that $x^2 - 2$ is indeed the minimal polynomial of $\sqrt{2}$ or that $x^2 + 1$ is indeed the minimal polynomial of i (once you prove that neither 2 nor -1 has a square root in $\mathbb{Q}$).

Example 5.49. For a cubic example, note that 2 has no cube root in $\mathbb{Q}$, so $x^3 - 2$ is irreducible in $\mathbb{Q}[x]$, hence $x^3 - 2$ is the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$.

Example 5.50. Note that $x^3 - 2$ is reducible in $\mathbb{R}[x]$, so it is not the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{R}$. In fact, over $\mathbb{R}[x]$, we have the factorization $x^3 - 2 = (x^2 + \sqrt[3]{2}x + \sqrt[3]{4})(x - \sqrt[3]{2})$, yet the polynomial $x^2 + \sqrt[3]{2}x + \sqrt[3]{4}$ is irreducible over $\mathbb{R}$ (i.e., in $\mathbb{R}[x]$) because it has no real roots.

Note that there are reducible quartic polynomials with no root in F. For an easy example, take $(x^2 - 2)^2$ for $F = \mathbb{Q}$.

6 Material Beyond Our Course

6.1 Toward Galois Theory

6.1.1 Degree of a Field Extension

Definition 6.1. Let E/F be a field extension. Then a *basis* of E over F is a subset $\{x_1, \cdots, x_n\} \subseteq F$ such that every $x \in E$ can be uniquely expressed as a linear combination

$$\lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_n x_n$$

for $\lambda_i \in F$.

Definition 6.2. We say that an extension E/F is *finite* if it has a finite basis. The *degree* of a finite extension E/F, denoted $[E : F]$, is the size of the basis. (Note: it is a theorem that this size does not depend on which basis one chooses.)

Given an extension, how can one determine its degree? It should be clear that $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ has degree 2 over $\mathbb{Q}$. We also know that $[E : F] = 1$ if and only if $E = F$. The following fact is helpful:

Fact 6.3. If $\alpha \in E$ is algebraic over F, then $F[\alpha]/F$ is a finite extension whose degree is the degree of the minimal polynomial of α over F.

More concretely, if that degree is n, then one can choose $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ as a basis.

For a more complicated field extension like $E = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$, there are a couple of approaches. One could try to show that in this case, $E = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}$ and that this representation is unique. Or, one could show that $E = \mathbb{Q}[\sqrt{2} + \sqrt{3}]$ as in one of the homework problems, and then show that $\sqrt{2} + \sqrt{3}$ has minimal polynomial $x^4 - 10x^2 + 1$ over $\mathbb{Q}$.

An even better way is to use the following proposition:

Fact 6.4. If $E/K/F$ is a sequence of (finite) field extensions, then $[E : F] = [E : K][K : F]$.

The proof proceeds by taking a basis $x_1, \cdots, x_n$ of E over K and a basis $y_1, \cdots, y_m$ of K over F and then showing that the set of mn products $\{x_i y_j\}$ is a basis for E over F.

The notion of degree of a field extension is the key to showing that one cannot construct, for example, a septagon, using ruler and compass. The idea is this: whenever one does a ruler and compass construction, the coordinates of the points one can construct can be found by addition, multiplication, subtraction, division, and square roots (because of the distance formula in Cartesian geometry, and because ruler and compass construction is all about drawing circles!). This means that they all lie in a field extension of $\mathbb{Q}$ given by taking square roots; by applying Fact 6.4 over and over, one sees that such an extension must have degree a power of 2.

Note that any divisor of a power of 2 is also a power of 2. Thus any *subfield* of such a field extension would also have degree a power of 2 by Fact

6.4. However, the number $\cos\frac{2\pi}{7}$ has minimal polynomial $x^3 + \frac{x^2}{2} - \frac{x}{2} - \frac{1}{8}$, which has degree 3. Therefore, $\mathbb{Q}[\cos\frac{2\pi}{7}]$ has degree 3 over $\mathbb{Q}$, so it cannot be contained in a field extension of $\mathbb{Q}$ whose degree is a power of 2.

6.1.2 Galois Theory

Given a polynomial $f(x) \in F[x]$, one can define the *splitting field* E_f of $f(x)$ over F. It is a field obtained by "adjoining" (inside some larger field, such as $\mathbb{C}$) all the roots of $f(x)$ to F. In other words, it is the smallest field E in which $f(x)$ *splits* into linear factors in $E[x]$.

One then defines the *Galois group* $\mathrm{Gal}(E_f/F)$ of $f(x)$ over F to be the group of automorphisms of the field E_f that act as the identity on F.

Note that if $\sigma \in \mathrm{Gal}(E_f/F)$, $\alpha \in E_f$, and $g(x) \in F[x]$, then $\sigma(g(\alpha)) = g(\sigma(\alpha))$ (this is an exercise in the definition of a ring homomorphism and of a polynomial!). In particular, if α is a root of $f(x)$, then $\sigma(\alpha)$ is also a root of $f(x)$. In particular, the elements of $\mathrm{Gal}(E_f/F)$ *permute* the roots of $f(x)$. If we let Z denote the set of roots of $f(x)$, then $\mathrm{Gal}(E_f/F)$ is a subgroup of $\Sigma(Z)$. For example, if $f(x)$ is a quintic polynomial with distinct roots, then $\mathrm{Gal}(E_f/F)$ is a subgroup of Sym_5.

A basic result of Galois says that $\mathrm{Gal}(E_f/F)$ acts transitively on the set of roots. The philosophy behind this is that any two roots "look the same algebraically, from the viewpoint of F."

Here are some examples:

Example 6.5. If $n \in \mathbb{Z}$ is not a square, then $\mathbb{Q}[\sqrt{n}]/\mathbb{Q}$ has Galois group of order 2. The non-identity element corresponds to the automorphism $a + b\sqrt{n} \mapsto a - b\sqrt{n}$.

Example 6.6. We can do the previous example over $\mathbb{R}$ instead of $\mathbb{Q}$ if n is negative, to get the extension $\mathbb{C}/\mathbb{R}$. The Galois group is once again size 2, and the non-trivial automorphism (i.e. non-identity element of the group) is complex conjugation.

Example 6.7. The field $\mathbb{Q}[\sqrt[3]{2}]$ is not a splitting field, because $\sqrt[3]{2}$ is not the *only* root of the polynomial $x^3 - 2 \in \mathbb{Q}[x]$. In fact, we have to all add the roots $\omega\sqrt[3]{2}$ and $\omega^2\sqrt[3]{2}$, where $\omega = \dfrac{-1+i\sqrt{3}}{2}$ is a primitive third root of unity. The field $\mathbb{Q}[\sqrt[3]{2}, \omega]$ is the splitting field of $x^3 - 2$ over $\mathbb{Q}$. In this case, there are three roots, and the Galois group is the full symmetric group Sym_3. This is an example of a *non-abelian* Galois group.

To learn more about Galois theory, pick up any text on abstract algebra, search "Galois theory notes" on Google, or see my notes at `https://math.berkeley.edu/~dcorwin/files/galoisthy.pdf`.

One set of notes I particularly like are those of Miles Reid at `https://homepages.warwick.ac.uk/~masda/MA3D5/Galois.pdf`. He has a really nice introductory section that explains the cubic and quartic formulas in light of the philosophy of Galois theory, so it really helps motivate Galois theory. Or see my account of the same topic at `https://math.berkeley.edu/~dcorwin/files/symmetry_cubic.pdf`.

You can also find some short articles about topics in Galois theory at `https://kconrad.math.uconn.edu/blurbs/`.

6.2 Algebraic Geometry

Algebraic geometry is a very important field of mathematics that has influenced many other fields, ranging from number theory to mathematical physics, and even to computer engineering.

Algebraic geometry is, on its surface, the study of solutions to polynomial equations in multiple variables. More specifically, it is the study of the relationship between solution sets of polynomials in multiple variables (geometry) and the ring theory of certain rings (algebra).

How does one associate a ring to a system of polynomial equations? Let's say $f_1(x_1, \cdots, x_n), \cdots, f_m(x_1, \cdots, x_n)$ is collection of m polynomials in n

variables with coefficients in a field F. We define the solution set or *variety* defined by $f_1, \cdots, f_m$ to be the set

$$V(f_1, \cdots, f_m) = \{(x_1, \cdots, x_n) \in F^n \mid f_i(x_1, \cdots, x_n) = 0 \, \forall \, i = 1, \cdots, m\}.$$

Then one associates the ring

$$A = A(V(f_1, \cdots, f_m)) \coloneqq F[x_1, \cdots, x_n]/(f_1, \cdots, f_m).$$

The idea is that the polynomials $f_1, \cdots, f_m$ are zero as functions on $V(f_1, \cdots, f_m)$, so we should mod out by them.

The ring $A(V(f_1, \cdots, f_m))$ is known as the *affine coordinate ring* of the variety. Algebraic geometers in the first half of the 20th century made the important observation that geometric properties of $V(f_1, \cdots, f_m)$ are equivalent to certain algebraic properties of the ring A. Here are three examples of this phenomenon:

If F is algebraically closed, then Hilbert's Nullstellensatz says that there's a natural bijection between the points of $V(f_1, \cdots, f_m)$ and the maximal ideals of the ring A.

If the variety is smooth (this means that the Jacobian of partial derivatives of the map from F^n to F^m defined by the polynomials f_i has full rank at every point of $V(f_1, \cdots, f_m)$, so that one may apply the implicit function theorem), then A is a UFD.

Finally, the ring A is an integral domain if and only if the variety is *irreducible*, which roughly means that it cannot be broken down as a union of smaller varieties. For example, the variety defined by the single equation $x_1 x_2 = 0$ is reducible, because it is the union of the variety defined by $x_1 = 0$ and the variety defined by $x_2 = 0$. Indeed, notice that $F[x_1, x_2]/(x_1 x_2)$ is not an integral domain.

The book `https://www.amazon.com/Invitation-Algebraic-Geometry-Universitext/dp/0387989803` is a wonderful introduction to algebraic geometry. You can probably even start reading this book just with the background you learned in this class!

6.3 p-adic Numbers

Check out `http://www.maths.gla.ac.uk/~ajb/dvi-ps/padicnotes.pdf` to learn about p-adic numbers. These also show up in a more advanced algebraic number theory course or in a commutative algebra course.

However, the basics of p-adic numbers are not too difficult, and I recommend learning about them now!

6.4 Algebraic Number Theory

Galois theory studies fields, especially fields of the form $\mathbb{Q}[\alpha]$, where $\alpha \in \mathbb{C}$ is some algebraic number. Because $\mathbb{Q}[\alpha]$ is a field, every nonzero element divides every other element, so divisibility isn't interesting. Similarly, every ideal is either $\{0\}$ or the whole ring, so the theory of ideals is not interesting.

On the other hand, if we consider $\mathbb{Z}[\alpha]$, divisibility and ideals are both much more interesting. For example, we might consider rings of the form $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{-5}]$, and more. We might ask whether or not they are UFD or PID. Algebraic number theory studies questions like these.

Remark 6.8. In general, we never have a chance of getting a UFD unless we take the *ring of integers*. Concretely, this means that in the field $\mathbb{Q}[\sqrt{5}]$, we must take the ring $\mathbb{Z}\left[\frac{\sqrt{5}+1}{2}\right]$ instead of the seemingly obvious $\mathbb{Z}[\sqrt{5}]$. More generally, if $K = \mathbb{Q}[\alpha]$, we define

$$\mathcal{O}_K \coloneqq \{\beta \in K \mid \beta \text{ is the root of a monic polynomial with integer coefficients.}\}.$$

Then $\mathcal{O}_K$ is known as the *ring of integers* of K, and it is a subring of K whose field of fractions is K.

Usually, people take a course titled "Algebraic Number Theory" or "Number Fields" after taking a course in Galois theory. However, there's a lot that you can learn before taking a full course in Galois theory. You can especially

study quadratic integer rings, as the Galois theory in that case is very simple (it is just conjugation). The quadratic integer rings take the form

$$\mathbb{Z}[\sqrt{d}]$$

if $d \equiv 2, 3 \pmod 4$. If $d \equiv 1 \pmod 4$, then $x^2 - x - \frac{d-1}{4}$ is monic polynomial with integer coefficients with roots $\frac{1 \pm \sqrt{d}}{2}$, so

$$\mathcal{O}_{\mathbb{Q}[\sqrt{d}]} = \mathbb{Z}\left[\frac{\sqrt{d}+1}{2}\right]$$

if $d \equiv 1 \pmod 4$, for d a squarefree integer. To read more about quadratic integer rings, check out `https://kconrad.math.uconn.edu/blurbs/gradnumthy/quadraticgrad.pdf` or Chapter 13 of Algebra by Michael Artin. These are sources you should be able to read now.

For even more material, you can look at `https://kconrad.math.uconn.edu/blurbs/`. For example, `https://kconrad.math.uconn.edu/blurbs/gradnumthy/dedekindf.pdf` introduces the idea that we should factor into ideals rather than elements, and `https://kconrad.math.uconn.edu/blurbs/gradnumthy/idealfactor.pdf` proves some basic facts about factorization of ideals. Some standard introductory textbooks on algebraic number theory are `https://www.springer.com/gp/book/9783319902326` and `https://www.maa.org/press/maa-reviews/algebraic-theory-of-numbers`.

6.5 Commutative Algebra

If you want to learn even more about the general theory of commutative rings, check out `http://www.math.toronto.edu/jcarlson/A--M.pdf`.

Generally, commutative algebra is seen more as a *tool* for subjects like algebraic number theory and algebraic geometry than as a subject in itself. Therefore, some people find it too abstract to learn before learning more about algebraic number theory and algebraic geometry for context - especially because algebraic geometry gives geometric intuition for concepts in

commutative algebra. On the other hand, some people may like to learn abstract theory before learning how to apply it.