MAT 333, Abstract Algebra

Serban Raianu
California State University, Dominguez Hills

Introduction

> "Young man, in mathematics you don't understand things. You just get used to them."
>
> John von Neumann

Algebra is the language of modern mathematics, so learning it can be frustrating and rewarding, just like learning a foreign language. If you have never tried to learn a foreign language as an adult imagine this: you are in a foreign country and you decided to learn the language. You bought a book with a CD and a TV. You already read the book and listened to the CD several times. You are watching the weatherman on TV, and you are sure he is saying some numbers, because the screen is full of them. Even though you can say and spell all numbers, you are not able to identify even a single one in what he is saying. Then you are watching the news and you see the prime minister on the screen. You know his name and you are sure the anchor must be saying his name but you could not identify the moment when she says it even if your life depended on it. Shortly put, you think you gave it your best effort but you don't understand anything. You feel like crying, and breaking the screen of your TV with your CD player. But you don't give up, and continue to work hard, read the book, listen to the CD, do the exercises, and watch TV. And one day, as if someone flipped a switch, your hard work pays off, and you are not only able to identify a temperature or a name, but you understand whole phrases. It feels like you are on top of the world.

In exactly the same way, when learning algebra, you will not be able to recognize for a while known terms in new contexts. Be prepared for this and keep trying, one day everything will click into place and its beauty will be revealed.

The other thing that makes studying algebra hard is developing an intuition when dealing with abstract notions, which can be hard. Acquiring it involves a lot of trial and error on concrete examples, which will need to be kept in our minds as a substitute of the abstract notion until the intuition becomes reliable, and we can reason on the abstract notion itself. Think of trying to study dogs in general (or an abstract dog) when all you know is your own dog. You will probably make an assertion on the abstract dog based on your own dog that will be false (say your dog is a Siberian Husky, and your claim is that all dogs have eyes of different colors). Understanding that the assertion is false means finding an example of another dog for which the assertion is false (this is called a counterexample, say you discover your neighbor has a Standard Poodle with eyes of the same color). From now on, the role of the abstract dog in your mind is played by a list of two dogs: your dog, which is an example for which the assertion is true, and the new dog, the counterexample (note that for the assertion "all dogs have eyes of the same color", your dog is the counterexample and the neighbor's dog is the example; this assertion is also false). You continue working, making assertions, trying to find examples, trying to prove the assertions, trying to find counterexamples when you can't prove the assertions, and so on. The abstract "dogs" that we study in algebra are the sets, groups, rings, fields, and so on. Imagine now that the only ring you know is the ring of integers, $\mathbb{Z}$. When you think of an abstract ring, you think of $\mathbb{Z}$. Based on your knowledge of $\mathbb{Z}$, you claim that in an abstract ring the product of two nonzero elements is nonzero. Then you discover that in the ring $\mathbb{Z}_4$ you have $2 \cdot 2 = 0$. From now on, when you think of an abstract ring you think of $\mathbb{Z}$ or $\mathbb{Z}_4$. Now based on your knowledge of $\mathbb{Z}$ and $\mathbb{Z}_4$ you claim that in a ring multiplication is commutative. Then you discover that in the ring of two by two matrices, $M_2(\mathbb{Z})$, multiplication is not commutative. From now on, when you think of an abstract ring you think of $\mathbb{Z}$, $\mathbb{Z}_4$, or $M_2(\mathbb{Z})$. To see if a new assertion on an abstract ring is true or not, you will first test it on these three rings. The list we are developing is a list of examples and counterexamples. Imagine a successful algebra student as a construction worker with tools conveniently arranged all over the body: the tools are the examples and counterexamples that help build our understanding of the abstract notions.

Our initial examples, the "dogs" that we "own" (i.e. the concrete examples we are supposed to know) are the number sets together with their operations. We assume we know that all the properties of the addition and multiplication of numbers are true, we will not prove them, and we will use them when needed. Understanding how we can construct a number set starting from another is an important part of the study of algebra:
We consider first the natural numbers

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$$

An equation of the type $m + x = n$ where $m, n \in \mathbb{N}$ might have a solution in $\mathbb{N}$, like $1+x=2$, or not, like $2+x=1$. By adding the solutions of all these equations to $\mathbb{N}$ we obtain the integers

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

Trying to make sense of the negative numbers that were added to $\mathbb{N}$ is not hard: we can think of positive and negative temperatures, going left or right on a line, receiving and giving (money), and so on.
Now an equation of the type $mx = n$ where $m, n \in \mathbb{Z}$ might have a solution in $\mathbb{Z}$, like $1 \cdot x = 2$, or not, like $2x = 1$. By adding the solutions of all these equations to $\mathbb{Z}$ we obtain the rationals

$$\mathbb{Q} = \left\{ \frac{m}{n} \mid m, n \in \mathbb{Z}, n \neq 0 \right\}$$

Again, trying to understand what $\frac{1}{2}$ means is not hard, think of a half of a pie. In this course we will learn how to perform a general construction of this type (see the section on Rings of Fractions).
Now an equation of the type $x^2 = m$ where $m \in \mathbb{Q}$ might have solutions in $\mathbb{Q}$, like $x^2 = 1$, or not, like $x^2 = 2$. Adding to $\mathbb{Q}$ all solutions of these equations (and also other numbers) leads to the reals $\mathbb{R}$. Making sense of $\sqrt{2}$ again is not hard: the diagonal of a square with side 1 has length $\sqrt{2}$.
Consider now an equation of the type $x^2 = r$ where $r \in \mathbb{R}$. This equation might have solutions, like $x^2 = 1$, or not, like $x^2 = -1$. Adding to $\mathbb{R}$ the solutions of this last equation, call them i and $-i$, leads to the complex numbers

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$$

Making sense of i took some time. Trying $i = \sqrt{-1}$ is a risky idea, because this radical does not have the same properties as the one we know. Assuming it does can lead to

$$-1 = i^2 = \sqrt{-1}\sqrt{-1} = \sqrt{(-1)^2} = \sqrt{1} = 1,$$

and warns us that if we do that we have to unlearn the property of radicals saying that $\sqrt{a}\sqrt{b} = \sqrt{ab}$. Failure to understand i is illustrated by the letter i (for "imaginary") used (sometimes with a derogatory connotation) to denote it. Algebra helps describe i precisely: as we will see later in this course, i is "the coset of the indeterminate in the factor ring of the polynomial ring in one indeterminate X with real coefficients factored through the principal ideal generated by the polynomial X^2+1." Therefore, we will learn in this course that we can construct $\mathbb{C}$ like this:

$$\mathbb{C} \simeq \mathbb{R}[X]/(X^2+1).$$

It may be interesting to note that we can no longer expand $\mathbb{C}$ by adding roots of polynomials with coefficients in $\mathbb{C}$: any polynomial of degree at least one with complex coefficients has a complex root in $\mathbb{C}$ (this is the famous Fundamental Theorem of Algebra and it says that $\mathbb{C}$ is algebraically closed).

There is yet another (fairly easy and convincing) justification for the "existence" of i, or at least of a model of it. We start with the matrix of the rotation of angle α about the origin in the plane:

$$\begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}$$

If we replace now $\cos(\alpha)$ and $\sin(\alpha)$ by $a, b \in \mathbb{R}$, we get

$$\left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \middle| a, b \in \mathbb{R} \right\} = \left\{ a \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \middle| a, b \in \mathbb{R} \right\}. \tag{1}$$

As we can easily check, we have

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \tag{2}$$

so if we define addition and multiplication in the set described in (1) by extending multiplication of real numbers and/or matrices, we see that the elements of this set behave exactly like the complex numbers. Then i may be seen as the rotation of 90° about the origin in the plane, and the equality $i^2 = -1$ can be read as "the rotation of 180° about the origin in the plane can be obtained by applying twice the rotation of 90°".

From a strictly algebraic point of view, the description of $\mathbb{C}$ as a factor ring is more valuable, because it uses a standard procedure for finding roots of polynomials. This course will expose mathematics majors to some other standard constructions and ideas of algebra. One of them is the principle according to which we try to describe various notions and constructions without referring to elements, but using only objects and maps (morphisms) between them. One of the benefits of this approach is that we can then easily move from sets (no operations) to groups (one operation) and to rings (two operations).

Other standard constructions that students will learn in this course are the notions of factor set (factor group, factor ring), ring of formal power series, and ring of polynomials. All these constructions satisfy certain "universal properties", which can be regarded as "apps" that are used to produce maps (or morphisms). The initial occurrence of a universal property is naturally explained by the attempt to describe a factor set using only sets and functions (and no elements), as mentioned above. The future math teachers will especially benefit from studying all these constructions, for example they will learn, among other things, the distinction between polynomials and polynomial functions.

Contents

Chapter 1

Part I

1.1 Lecture 1.1: Sets and functions, 1

No communication is possible without a common ground consisting of terms that everybody understands. In the absence of these terms it is not even possible to ask questions. One such primary notion, which we assume we all know, is the notion of a set. Sets consist of elements. We write that a is an element of the set A like this: $a \in A$. A set A is a subset of the set B if every element of A is also an element of B, and we write this as $A \subseteq B$. We denote by $\emptyset$ the empty set, the set with no elements. The set whose elements are $a_1, a_2, \ldots a_n$ will be denoted by $\{a_1, a_2, \ldots a_n\}$. The union of the sets A and B consists of the elements that belong to at least one of the sets:

$$A \cup B = \{a \mid a \in A \text{ or } a \in B\}.$$

The intersection of the sets A and B consists of the elements that belong to both sets:

$$A \cap B = \{a \mid a \in A \text{ and } a \in B\}.$$

Basic examples of sets include sets of numbers: the natural numbers $\mathbb{N} = \{0, 1, 2, \ldots\}$, the integers $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$, the rationals $\mathbb{Q} = \{\frac{m}{n} \mid m, n \in \mathbb{Z}, n \neq 0\}$, the real numbers $\mathbb{R}$, and the complex numbers $\mathbb{C}$.

Assuming we all know something that we do not completely understand is risky. To see that this naive approach may lead to paradoxes consider the set of all sets and denote it by $\mathcal{S}$. Then let $M = \{X \in \mathcal{S} \mid X \notin X\}$, and we see that $M \in M$ if and only if M itself satisfies the condition in the definition of M, which is $M \notin M$. Paradoxes like this one have prompted various attempts to introduce sets by a list of axioms.

Once we know what a set is we can define ordered pairs of elements: (x, y) will mean the set $\{\{x, y\}, \{x\}\}$, i.e. x and y are the elements, order matters and x is the first element. Note that $\{1, 2\} = \{2, 1\}$ because the two sets have the same elements, but $(1, 2) \neq (2, 1)$ because the sets $\{\{1, 2\}, \{1\}\}$ and $\{\{1, 2\}, \{2\}\}$ do not have the same elements. The cartesian product of the sets A and B is defined by

$$A \times B = \{(a, b) \mid a \in A, \ \ b \in B\}$$

We can now give the definition of a function (or map):

Definition 1.1.1 *A function f defined on A with values in B (we write $f : A \longrightarrow B$ and we say that f is defined on A with values in B) consists of three sets: A, the domain; B, the codomain; and a subset G_f of $A \times B$, the graph, satisfying the property that for every $a \in A$ there is a unique $b \in B$ such that $(a, b) \in G_f$. If $(a, b) \in G_f$ we write $b = f(a)$ and call it the image of a through f.*

Two functions are equal if all three pairs of sets in the definition are equal: the functions have the same domain, the same codomain, and the images of every element in the common domain through the two functions are also equal. If $f : A \longrightarrow B$ and $g : B \longrightarrow C$, then we can define the composition of the functions f and g by $g \circ f : A \longrightarrow C$, $(g \circ f)(a) = g(f(a))$ for all $a \in A$. Sometimes we write gf instead of $g \circ f$.

Proposition 1.1.2 *If $f : A \longrightarrow B$, $g : B \longrightarrow C$ and $h : C \longrightarrow D$, prove that $(h \circ g) \circ f = h \circ (g \circ f)$. (We say that the composition of functions is associative.)*

Proof: Both $(h \circ g) \circ f$ and $h \circ (g \circ f)$ have domain A and codomain D, so we only need to show that $((h \circ g) \circ f)(a) = (h \circ (g \circ f))(a)$ for all $a \in A$. If $a \in A$, then $((h \circ g) \circ f)(a) = (h \circ g)(f(a)) = h(g(f(a))) = h((g \circ f)(a)) = (h \circ (g \circ f))(a)$. ∎

If $f : A \longrightarrow B$ is a function, $C \subseteq A$ and $D \subseteq B$, we define the image of C through f as

$$f(C) = \{f(a) \mid a \in C\},$$

and the preimage (inverse image) of D through f as

$$f^{-1}(D) = \{a \mid a \in A, \ \ f(a) \in D\}.$$

We call $f(A)$ the range (or the image) of the function f and we denote it by $Im(f)$.

Given any set A, the identity function of the set A, denoted Id_A or 1_A, is the function defined on A with values in A that sends each element $a \in A$ to itself: $Id_A : A \longrightarrow A$, $Id_A(a) = a$ for all $a \in A$.

1.2 Lecture 1.2: Sets and functions, 2

We define the following special classes of functions:

Definition 1.2.1 *We say that the function $f : A \longrightarrow B$ is injective (or one-to-one) if $f(a_1) = f(a_2)$ implies that $a_1 = a_2$, or, equivalently, if $a_1 \neq a_2$ implies that $f(a_1) \neq f(a_2)$.*

Definition 1.2.2 *We say that the function $f : A \longrightarrow B$ is surjective (or onto) if for any element $b \in B$ there exists $a \in A$ such that $b = f(a)$, or, equivalently, if $Im(f) = B$.*

Definition 1.2.3 *A function that is both injective and surjective is called bijective.*

Proposition 1.2.4 *Let $f : A \longrightarrow B$ and assume that $A = \{a_1, a_2, \dots, a_n\}$, $B = \{b_1, b_2, \dots, b_n\}$. If f is injective or surjective, then f is bijective.*

Proof: If f is injective, $Im(f)$ has n elements and is contained in B, which also has n elements, therefore $Im(f) = B$ and f is surjective. If f is surjective but not injective, $Im(f)$ has at most $n - 1$ elements, a contradiction. ∎

For the rest of this lecture we will assume that all sets are nonempty. Our next goal is to show that the notions of injective and surjective functions are really similar, which is something that we cannot see by comparing Definitions 1.2.1 and 1.2.2.

Proposition 1.2.5 *Let $f : A \longrightarrow B$ be a function. Then the following assertions hold:*
i) f is injective if and only if there exists a function $g : B \longrightarrow A$ such that $g \circ f = Id_A$, i.e. f has a left inverse.
ii) f is surjective if and only if there exists a function $g : B \longrightarrow A$ such that $f \circ g = Id_B$, i.e. f has a right inverse.

Proof: i) Assume f is injective, and fix an element $a_0 \in A$. We define g as follows: if $b \in B$ is not in $Im(f)$, set $g(b) = a_0$. If $b \in Im(f)$, since f is injective there exists a unique $a \in A$ such that $b = f(a)$. In this case let $g(b) = a$. Then for each $a \in A$ we have that $g(f(a)) = a$, so $g \circ f = Id_A$. Conversely, if a function $g : B \longrightarrow A$ such that $g \circ f = Id_A$ exists, let $f(a_1) = f(a_2)$. Then $g(f(a_1)) = g(f(a_2))$, and so $a_1 = a_2$.
ii) Assume f is surjective, and let $b \in B$. Then we choose an element $a \in A$ such that $f(a) = b$ (which exists because f is surjective) and we let $g(b) = a$. Then $f(g(b)) = f(a) = b$, so $f \circ g = Id_B$. Conversely, if a function $g : B \longrightarrow A$ such that $f \circ g = Id_B$ exists, then for any $b \in B$ we have that $b = f(g(b))$, so $b \in Im(f)$ and thus f is surjective. ∎

Proposition 1.2.5 shows that injectivity and surjectivity are closely related, we can get one from the other by replacing "left" with "right" or the other way around. It also provides the following useful characterization of bijective functions:

Corollary 1.2.6 *A function $f : A \longrightarrow B$ is bijective if and only if it is invertible, i.e. there exists a function $g : B \longrightarrow A$ such that $f \circ g = Id_B$ and $g \circ f = Id_A$.*

Proof: If f is bijective, then by Proposition 1.2.5 it has a left inverse g_1 and a right inverse g_2. Then for any $b \in B$ we have that $g_1(b) = g_1(Id_B(b)) = g_1(f \circ g_2(b)) = (g_1 \circ f)(g_2(b)) = Id_A(g_2(b)) = g_2(b)$, so $g_1 = g_2$, and f is invertible. The converse follows immediately from Proposition 1.2.5. ∎

As seen in the proof above, a function cannot have more than one inverse: if the inverse exists it must be unique, and our notation for it will be f^{-1}. Note that this notation makes sense even if f is not invertible (the preimage of a subset above), but in case the function is invertible, the preimage of a subset is the image of that set through the inverse function, which justifies the notation.

Proposition 1.2.7 *Prove that the inverse of a bijective function is also bijective.*

Proof: The inverse of a bijective function is invertible, and is therefore bijective by Corollary 1.2.6. ∎

Proposition 1.2.8 *If $f : A \longrightarrow B$ and $g : B \longrightarrow C$ are injective functions, then $g \circ f$ is also injective. The assertion is also true if we replace "injective" by "surjective".*

Proof: If f and g are injective, let f_1 and g_1 be left inverses of f and g, respectively. Thus $f_1 : B \longrightarrow A$, $g_1 : C \longrightarrow B$, $f_1 \circ f = Id_A$ and $g_1 \circ g = Id_B$. We have that $(f_1 \circ g_1) \circ (g \circ f) = f_1 \circ (g_1 \circ g) \circ f = f_1 \circ Id_B \circ f = f_1 \circ f = Id_A$, so $f_1 \circ g_1$ is a left inverse of $g \circ f$, and thus $g \circ f$ is injective. The proof for the case of surjective functions is similar. ∎

Proposition 1.2.9 *If $f : A \longrightarrow B$ and $g : B \longrightarrow C$ are functions such that $g \circ f$ is injective, then f is injective.*

Proof: Let $e : C \longrightarrow A$ be a left inverse for $g \circ f$, i.e. $e \circ (g \circ f) = Id_A$. Then $e \circ g$ is a left inverse for f, so f is injective. ∎

Proposition 1.2.10 *If $f : A \longrightarrow B$ and $g : B \longrightarrow C$ are functions such that $g \circ f$ is surjective, then g is surjective.*

Proof: Let $e : C \longrightarrow A$ be a right inverse for $g \circ f$, i.e. $(g \circ f) \circ e = Id_C$. Then $f \circ e$ is a right inverse for g, so g is surjective. ∎

Proposition 1.2.11 *If $f : A \longrightarrow B$ is a function, $C_1, C_2 \subseteq A$, $D_1, D_2 \subseteq B$, then:*
i) $f(C_1 \cup C_2) = f(C_1) \cup f(C_2)$.
ii) $f(C_1 \cap C_2) \subseteq f(C_1) \cap f(C_2)$. Give an example when the inclusion is strict, and prove that if f is injective equality holds.
iii) $f^{-1}(D_1 \cup D_2) = f^{-1}(D_1) \cup f^{-1}(D_2)$.
iv) $f^{-1}(D_1 \cap D_2) = f^{-1}(D_1) \cap f^{-1}(D_2)$.

Proof: i) Let $b \in f(C_1 \cup C_2)$. Then $b = f(a)$, where $a \in C_1 \cup C_2$, i.e. $a \in C_1$ or $a \in C_2$. Then $b \in f(C_1)$ or $b \in f(C_2)$, so $b \in f(C_1) \cup f(C_2)$. Conversely, $f(C_1) \subseteq f(C_1) \cup f(C_2)$ and $f(C_2) \subseteq f(C_1) \cup f(C_2)$, so $f(C_1) \cup f(C_2) \subseteq f(C_1) \cup f(C_2)$.
ii) Let $b \in f(C_1 \cap C_2)$. Then $b = f(a)$, where $a \in C_1 \cap C_2$, i.e. $a \in C_1$ and $a \in C_2$. Then $b \in f(C_1)$ and $b \in f(C_2)$, so $b \in f(C_1) \cap f(C_2)$. Conversely, if $b \in f(C_1) \cap f(C_2)$, then $b = f(a_1)$, where $a_1 \in C_1$, and $b = f(a_2)$, where $a_2 \in C_2$. If f is injective, then we get that $a_1 = a_2$ so $b \in f(C_1) \cap f(C_2)$, and thus $f(C_1) \cap f(C_2) = f(C_1) \cap f(C_2)$. An example when the inclusion is strict is the following: $A = \{1, 2\}$, $B = \{1\}$, $f : A \longrightarrow B$, $f(1) = f(2) = 1$, $C_1 = \{1\}$, $C_2 = \{2\}$. Then $C_1 \cap C_2 = \emptyset$, so $f(C_1 \cap C_2) = \emptyset$, and $f(C_1) \cap f(C_2) = \{1\}$.
iii) We have that $a \in f^{-1}(D_1 \cup D_2)$ if and only if $f(a) \in D_1 \cup D_2$ if and only if $f(a) \in D_1$ or $f(a) \in D_2$ if and only if $a \in f^{-1}(D_1) \cup f^{-1}(D_2)$.
iv) We have that $a \in f^{-1}(D_1 \cap D_2)$ if and only if $f(a) \in D_1 \cap D_2$ if and only if $f(a) \in D_1$ and $f(a) \in D_2$ if and only if $a \in f^{-1}(D_1) \cap f^{-1}(D_2)$. ∎

Proposition 1.2.12 *Let $M = \{x_1, x_2, \ldots, x_m\}$ and $N = \{y_1, y_2, \ldots, y_n\}$.*
i) If $A_1, A_2, \ldots, A_k \in \mathcal{P}(M)$, prove by induction on k that

$$card(A_1 \cup A_2 \cup \ldots \cup A_k) = \sum_{i=1}^{k} card(A_i) - \sum_{1 \leq i < j \leq k} card(A_i \cap A_j) +$$

$$+ \ldots + (-1)^{k+1} card(\cap_{i=1}^{k} A_i)$$

(This is the inclusion-exclusion principle)
ii) The number of functions from M to N is n^m.
iii) $card(\mathcal{P}(M)) = 2^m$.
iv) If $m = n$, the number of bijective functions from M to N is $m!$.
v) If $m \leq n$, the number of injective functions from M to N is ${}_nP_m = \frac{n!}{(n-m)!}$.

vi) If $m \geq n$, the number of surjective functions from M to N is:

$$n^m - \binom{n}{1}(n-1)^m + \binom{n}{2}(n-2)^m + \ldots + (-1)^{n-1}\binom{n}{n-1},$$

where $\binom{n}{k} = {}_nC_k = \dfrac{n!}{k!(n-k)!}$.

Proof: i) For $k = 2$ the assertion is clear, just note that when you add the number of elements of A_1 and A_2, the elements in the intersection are counted twice. Assume now that $k > 2$ and the assertion is true for $k-1$ sets. Then we have

$$(A_1 \cup A_2 \cup \ldots \cup A_{k-1}) \cap A_k = \cup_{i<k}(A_i \cap A_k),$$

so applying the case $k = 2$ we get

$$card(A_1 \cup A_2 \cup \ldots \cup A_k) = card(A_1 \cup A_2 \cup \ldots \cup A_{k-1}) + card(A_k) -$$

$$-card(\cup_{i<k}(A_i \cap A_k)),$$

and we can apply the induction hypothesis and regroup the terms to get the assertion for k.

ii) We use induction on m. If $m = 1$, then M has one element, and it is clear that there are exactly n functions form M to N. If we assume that there are n^{m-1} functions from $\{x_1, \ldots, x_{m-1}\}$ to N, then each function from M to N can be obtained by extending one of those functions by defining it on x_m. Since this can be done in n ways, it follows that there are $n^{m-1} \cdot n = n^m$ functions from M to N.

iii) The function $\phi : \mathcal{P}(M) \longrightarrow \{0,1\}^M$, defined by

$$\phi(X)(x) = \begin{cases} 1 & \text{if } x \in X \\ 0 & \text{if } x \notin X \end{cases}$$

which is called the characteristic function of the subset X, is a bijection, with inverse $\psi : \{0,1\}^M \longrightarrow \mathcal{P}(M)$, defined by $\psi(f) = f^{-1}(1)$. Then the assertion follows from ii).

iv) To define a bijection from M to N, we can give it any value at x_1, then x_2 can be sent to any of the remaining $m-1$ values, and so on, until the value at x_m will be the only element of Y left available. So there are $m \cdot (m-1) \cdot \ldots \cdot 1 = m!$ bijective functions from M to N.

v) There is a bijection between the set in injective functions from M to N and the set of ordered subsets with m elements of N. Since there are $\binom{n}{m} = {}_nC_m = \dfrac{n!}{m!(n-m)!}$ subsets of N with m elements, and each set

can be ordered in $m!$ ways by iv), the number of injective functions from M to N is $m! \cdot {}_nC_m = {}_nP_m$.
vi) Let us denote by A_i the set of functions from M to N which do not take the value y_i. The set of functions that are not surjective is $A_1 \cup A_2 \cup \ldots \cup A_n$, so the number of surjective functions is $n^m - card(A_1 \cup A_2 \cup \ldots \cup A_n)$. But A_i is the set of functions from M to the set $N \setminus \{y_i\} = \{y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_n\}$, so $card(A_i) = (n-1)^m$, and therefore $\sum_{i=1}^n card(A_i) = n(n-1)^m$. Similarly, $A_i \cap A_j$ is the set of functions from M to $N \setminus \{y_i, y_j\}$, and so $card(A_i \cap A_j) = (n-2)^m$, and so $\sum_{i<j} card(A_i \cap A_j) = \binom{n}{2}(n-2)^m$, and so on. Note that $A_1 \cap A_2 \cap \ldots \cap A_n = \emptyset$. ∎

1.3 Lecture 1.3: The integers, 1

In this lecture we start reviewing the arithmetic properties of the integers. All letters in the next two lectures will represent integers. We will use the following

Well-Ordering Principle. Any nonempty set of nonnegative integers has a least element.

The first application of this principle is

Theorem 1.3.1 (The Division Algorithm) *If a and b are integers and $b \neq 0$, then there exist integers q and r such that $a = bq + r$ and $|r| < |b|$.*

Proof: We will find q and r satisfying the conditions, with $r \geq 0$. These q and r are usually called the quotient and remainder of a divided by b.
Consider the set $W = \{a - tb \geq 0 \mid t \in \mathbb{Z}\}$. It is easy to see that W is nonempty, just take $t = -|a|\, b$. By the well-ordering principle, W has a least element $r = a - qb$. We claim that $r < |b|$. Indeed, if $|b| \leq r$, then $r > r - |b| \geq 0$, and $r - |b| = a - qb - |b| = a - (q \pm 1)b \in W$, which contradicts the fact that r is the least element in W.
Finally, we remark that if $r \neq 0$, the pair $q + \frac{|b|}{b}$ and $r - |b|$ also satisfy the conditions. ∎

As we can see from the proof, we might get two pairs of quotients and remainders. If in the the homework problems on WeBWorK you are asked to find one quotient and one remainder it means that you are asked to provide the pair with the positive remainder. Here's a quick way to apply the division algorithm for two numbers a and b using a calculator: if a and b are positive, divide a by b on the calculator. Denote by q the greatest integer less than the result, and find r as $r = a - bq$. In case one or both of a and b are negative, do the above using their absolute values, then adjust your answer accordingly.

Theorem 1.3.1 has important practical consequences. For example it says that any integer has one of the forms $2k$ or $2k + 1$.

Definition 1.3.2 *Given integers a and b, we say that a divides b (or a is a factor of b, or b is a multiple of a, or b is divisible by a), and we write $a \mid b$, if there exists an integer c such that $b = ac$.*

Proposition 1.3.3 *We have the following:*
i) $1 \mid a$ for all a.
ii) $a \mid 0$ for all a.
iii) If $a \mid b$ and $b \mid c$, then $a \mid c$.

iv) If $a \mid b$ and $c \mid d$, then $ac \mid bd$.
v) If $a \mid b$ and $a \mid c$, then $a \mid ub + vc$ for all u, v.
vi) If $a \mid 1$, then $a = \pm 1$.
vii) If $a \mid b$ and $b \mid a$, then $a = \pm b$.

Proof: i) $a = 1 \cdot a$.
ii) $0 = a \cdot 0$.
iii) We have that $b = ad$ and $c = be = ade$.
iv) We have that $b = ae$ and $d = cf$, so $bd = acef$.
v) We have $b = ad$ and $c = ae$, so $ub + vc = uad + vae = a(ud + ve)$.
vi) We have $1 = ab$, so $|a| = 1$.
vii) If both a and b are 0, the statement is clear. If one of them is not 0, the other one has to be different from 0 as well. In that case we have $b = au$ and $a = bv = auv$, so $1 = uv$. ∎

Definition 1.3.4 *Given integers a and b, we say that d is a* **greatest common divisor***(or greatest common factor) of a and b (we write $d = (a, b)$) if the following two conditions are satisfied:*
i) $d \mid a$ and $d \mid b$.
ii) if $c \mid a$ and $c \mid b$, then $c \mid d$.

It follows immediately from the definition that $a \mid b$ if and only if $a = (a, b)$.

Proposition 1.3.5 *If $d_1 = (a, b)$ and $d_2 = (a, b)$, then $d_1 = \pm d_2$.*

Proof: Since $d_1 = (a, b)$, $d_2 \mid a$, and $d_2 \mid b$, it follows that $d_2 \mid d_1$. Similarly, $d_1 \mid d_2$. ∎

A second application of the well-ordering principle is the existence of a greatest common divisor:

Theorem 1.3.6 *Given integers a and b, a greatest common divisor of a and b exists.*

Proof: If $a = b = 0$, then $0 = (0, 0)$. If not both of a and b are 0, consider the set $W = \{ma + nb > 0 \mid m, n \in \mathbb{Z}\}$. $W \neq \emptyset$ because $a^2 + b^2 \in W$. By the well-ordering principle W has a least element $d = ua + vb$, and we show that $d = (a, b)$. We prove first that $d \mid a$. Indeed, if d does not divide a we use the division algorithm to find q and r such that $a = dq + r$, where $0 < r < d$. Now since $r = a - dq = a - (ua + vb) = (1 - u)a + (-v)b \in W$, this contradicts the fact that d is the least element in W. The proof of the fact that $d \mid b$ is identical. Finally, if $c \mid a$ and $c \mid b$, then $a = ce$ and $b = cf$. It follows that $d = ua + vb = uce + vcf = c(ue + vf)$, so $c \mid d$ and the proof is complete. ∎

From the proof of Theorem 1.3.6 we immediately obtain the following

Corollary 1.3.7 *Given integers a and b, if $d = (a, b)$, then there exist u, v such that $d = ua + vb$. (We say that d is a linear combination of a and b.)*

Remark 1.3.8 *i) The following example shows that u and v in Corollary 1.3.7 are not unique: $1 = (2, 3)$, and $1 = 2 \cdot (-1) + 3 \cdot 1 = 2 \cdot 2 + 3 \cdot (-1)$.*
ii) We have that $d = ua + vb$ does not imply $d = (a, b)$, e.g. $2 = 1 \cdot 1 + 1 \cdot 1$.

Proposition 1.3.9 (The Euclidean Algorithm)
i) If $a = bq + r$, then $(a, b) = (b, r)$.
ii) If a, b are nonzero integers, consider the following chain of divisions:
$\mid a \mid = q_0 \cdot |b| + r_0$, *where* $0 \leq r_0 < |b|$,
$|b| = q_1 \cdot r_0 + r_1$, *where* $0 \leq r_1 < r_0$,
$r_0 = q_2 \cdot r_1 + r_2$, *where* $0 \leq r_2 < r_1$,
$\ldots$
$r_n = q_{n+2} \cdot r_{n+1} + r_{n+2}$, *where* $0 \leq r_{n+2} < r_{n+1}$,
$\ldots$
Then $\{r_n\}$ is a strictly decreasing chain of nonnegative integers, so one of them has to be 0. The last nonzero remainder in this chain is a greatest common divisor for a and b.

Proof: i) Let $d = (a, b)$. We show that $d = (b, r)$. We clearly have that $d \mid b$, and since $d \mid a$, we also get that $d \mid a - qb = r$, so d is a common divisor of b and r. Now if $c \mid b$ and $c \mid r$, we have that $c \mid bq + r = a$, so $c \mid d$.
Conversely, if $d = (b, r)$, we show that $d = (a, b)$. We clearly have that $d \mid b$, and since $d \mid r$, we also get that $d \mid bq + r = a$, so d is a common divisor of a and b. Now if $c \mid a$ and $c \mid b$, then $c \mid a - bq = r$, so $c \mid d$.
ii) Assume that r_n is the last nonzero term of the sequence of remainders, so $r_{n+1} = 0$. Applying i) repeatedly we get that $(\mid a \mid, \mid b \mid) = (\mid b \mid, r_0) = (r_0, r_1) = \ldots = (r_n, r_{n+1}) = (r_n, 0) = r_n$, so $r_n = (a, b)$. ∎

Remark 1.3.10 *If we find $d = (a, b)$ using the Euclidean algorithm, we can use back substitution to write d as a linear combination of a and b.*

Try the following exercise before doing your homework and without looking at the solution below.

Exercise 1.3.11 *Use the Euclidean algorithm to find $(987, -345)$, then write it as a linear combination of 987 and -345.*

Solution: Since $(987, -345) = (987, 345)$ we have:
$987 = 2 \cdot 345 + 297$, $0 \leq 297 < 345$
$345 = 1 \cdot 297 + 48$, $0 \leq 48 < 297$

$297 = 6 \cdot 48 + 9$, $0 \leq 9 < 48$
$48 = 5 \cdot 9 + 3$, $0 \leq 3 < 9$
$9 = 3 \cdot 3 + 0$. Then $3 = (987, 345)$, and $3 = 48 - 5 \cdot 9 = 48 - 5 \cdot (297 - 6 \cdot 48) = 31 \cdot 48 - 5 \cdot 297 = 31 \cdot (345 - 1 \cdot 297) - 5 \cdot 297 = 31 \cdot 345 - 36 \cdot 297 = 31 \cdot 345 - 36 \cdot (987 - 2 \cdot 345) = 103 \cdot 345 - 36 \cdot 987 = (-103) \cdot (-345) - 36 \cdot 987$.

1.4 Lecture 1.4: The integers, 2

In this lecture we continue reviewing the arithmetic properties of the integers. All letters in this lecture represent integers.

Definition 1.4.1 *We say that a and b are* **relatively prime** *if $1 = (a, b)$.*

Remark 1.4.2 *i) a and b are relatively prime if and only if $1 = ma + nb$ for some m and n. Indeed, if $1 = (a, b)$, then 1 is a linear combination of a and b by Corollary 1.3.7. Conversely, if $1 = ma + nb$, $d \mid a$ and $d \mid b$, it follows that $d \mid 1$.*
ii) If $0 \neq d = (a, b)$, $a = da_1$, $b = db_1$, then $1 = (a_1, b_1)$. To see this, write $d = au + bv = da_1u + db_1v$, divide by d, then apply i).

Theorem 1.4.3 (Euclid's Lemma) *If $1 = (a, b)$, and $a \mid bc$, then $a \mid c$.*

Proof: Write $1 = ma+nb$, and $bc = ae$. Then $c = mac+nbc = mac+nae = a(mc + ne)$. ∎

We recall now the definition of a least common multiple of two integers. (Note that the definition can be extended to any number of integers.)

Definition 1.4.4 *If a and b are integers, we say that m is a least common multiple of a and b (and we write $m = [a, b]$) if the following conditions hold:*
i) $a \mid m$ and $b \mid m$.
ii) If $a \mid n$ and $b \mid n$, then $m \mid n$.

Proposition 1.4.5 *If a and b are integers, then $ab = (a, b)[a, b]$ (this means that if not both of a and b are 0, then $[a, b] = ab/(a, b)$.)*

Proof: It is clear that $[0, 0] = (0, 0) = 0$. Now if a and b are not both 0, let $d = (a, b)$. We have that $d \mid a \mid ab$, so $ab = md$. We show that $m = [a, b]$. We have that $a = da_1$ and $b = db_1$. Therefore, $da_1db_1 = md$, hence $a_1db_1 = a_1b = ab_1 = m$, i.e. m is a multiple of a and b. Now if $a \mid n$ and $b \mid n$, it follows that $n = aa_2$ and $n = bb_2$, so $na_1 = ba_1b_2 = mb_2$, and $nb_1 = ab_1a_2 = ma_2$. Let u, v be such that $1 = ua_1 + vb_1$. Then $n = n(ua_1 + vb_1) = umb_2 + vma_2 = m(ub_2 + va_2)$. ∎

Definition 1.4.6 *An integer $p \neq 0$, $p \neq \pm1$, is said to be* **prime** *if from $p \mid ab$ it follows that $p \mid a$ or $p \mid b$.*

Proposition 1.4.7 *Let $p \neq 0$, $p \neq \pm1$. The following assertions are equivalent:*
i) p is prime.
ii) If $p = ab$, then one of a and b has the same absolute value as p.
iii) $d \mid p$ implies that $d = \pm1$ or $d = \pm p$.

Proof: *i*) $\Rightarrow$ *ii*). Since $p = ab$, it follows that $a \mid p$ and $b \mid p$, and also that $p \mid ab$. Since p is prime, it follows that $p \mid a$ or $p \mid b$. Therefore $a = \pm p$ or $b = \pm p$ by Exercise 1.3.3, *vii*).
ii) $\Rightarrow$ *iii*). Let $p = de$. It follows that $|d| = |p|$, in which case $d = \pm p$, or $|e| = |p|$, in which case $d = \pm 1$.
iii) $\Rightarrow$ *i*). Let $p \mid ab$, and consider $d = (a, p)$. From the hypothesis it follows that either $d = \pm 1$, in which case $p \mid b$ by Euclid's lemma, or $d = \pm a$, which means that $p \mid a$. ∎

Proposition 1.4.8 *If p is prime, and $p \mid a_1a_2 \ldots a_n$, then there exists i, $1 \leq i \leq n$ such that $p \mid a_i$.*

Proof: We use induction on n. If $n = 1$ there is nothing to prove. If $n > 1$ and the assertion is true for numbers $< n$, we have $p \mid a_1 \cdot (a_2 \ldots a_n)$, so either $p \mid a_1$ or $p \mid a_2 \ldots a_n$ and we can apply the induction hypothesis. ∎

The following important result is another application of the well-ordering principle.

Theorem 1.4.9 (Fundamental Theorem of Arithmetic) *Any integer $n \neq 0, \pm 1$ can be factored as a product of primes.(This means that if $n \neq 0, \pm 1$, then $n = p_1p_2 \ldots p_k$, where p_i is prime, $1 \leq i \leq k$.) Moreover, the factorization is unique if we disregard the order of the prime factors or their signs. (This means that if we have another factorization $n = q_1q_2 \ldots q_l$, where q_j is prime, $1 \leq j \leq l$, then $k = l$ and for any i, $1 \leq i \leq k$ there exists a j, $1 \leq j \leq k$ such that $p_i = \pm q_j$. Also, it follows that for any prime p, the number of primes associated in divisibility with p in any factorization of n as a product of primes does not depend of the factorization, and is equal to the maximum power of p that divides n.)*

Proof: We prove the assertion for integers grater than 1.
Let $W = \{n \mid n > 1, n \text{ cannot be factored as in the statement}\}$. By the well-ordering principle, if W is nonempty, then W has a least element m. Since $m \in W$ we have that m is not prime, so we can write $m = ab$, where $1 < a, b < m$. Since m is the least element of W it follows that none of a and b are elements of W, so both of them have a factorization as in the statement. But replacing those factorizations in $m = ab$ we see that m has one such factorization, a contradiction. Now for the uniqueness part, assume that

$$p_1p_2 \ldots p_k = q_1q_2 \ldots q_l$$

are two factorizations as products of primes, and we proceed by induction on the length of the factorization, which is the maximum of k and l. The case when the length is 1 is clear. Assume that the length is greater than

1 and the assertion is true for smaller lengths. Then $p_1 \mid q_1 q_2 \dots q_l$, and so p_1 divides one of the q_j. It follows that $p_1 = \pm q_j$, and after canceling p_1 we can apply the induction hypothesis. ∎

Remark 1.4.10 *Why do we ask $p \neq 0$, $p \neq \pm 1$ in Definition 1.4.6? While it is true that 0 satisfies the definition of prime numbers, and ± 1 satisfy the equivalent conditions in Exercise 1.4.7, accepting any of these three numbers as prime would hurt the uniqueness of the decomposition as a product of prime numbers in the fundamental theorem of arithmetic (Theorem 1.4.9).*

The following old result and its proof go back to Euclid.

Theorem 1.4.11 *There are infinitely many prime numbers.*

Proof: We assume that $p_1, p_2, \dots, p_n$ are all the prime numbers, and look for a contradiction. We let $n = 1 + p_1 p_2 \dots p_n$. Then $|p_1 p_2 \dots p_n| > 1$, so $n \neq 0$, $n \neq \pm 1$. By Theorem 1.4.9 there exists i, $1 \leq i \leq n$ such that $p_i \mid n$. Then $p_i \mid n - p_1 p_2 \dots p_n = 1$, a contradiction. ∎

Remark 1.4.12 *Theorem 1.4.9 can help shorten the proof of the fact that $\sqrt{2}$ is irrational, as you saw it in MAT 271. If p is prime, then we show that $\sqrt{p}$ is irrational by proving that there are no integers a and b such that $a^2 = pb^2$. Assuming that such a and b exist, and looking at maximum powers of p dividing both sides of the equality $a^2 = pb^2$, we see that the highest power of p dividing the left is even, while the maximum power of p dividing the right is odd, and this contradicts the uniqueness of the decomposition as a product of prime numbers in the fundamental theorem of arithmetic.*

We close this lecture with a nice application:

Proposition 1.4.13 *It is not possible to draw an equilateral triangle on graph paper such that all vertices are at nodes of the grid.*

Proof: Suppose such an equilateral triangle exists, and draw horizontal and vertical lines through the vertices of the triangle in order to inscribe it in a rectangle whose sides have integer lengths. This rectangle is the union of the equilateral triangle and two or three right triangles. Right triangles whose legs have integer lengths have rational areas (either an integer or half of an integer). Denote by l the side of the equilateral triangle. By the Pythagorean theorem, l^2 is an integer. It follows that the area of the triangle, which is $\frac{l^2\sqrt{3}}{4}$, is rational, so $\sqrt{3}$ is rational, a contradiction. ∎

1.5 Lecture 1.5: Equivalence relations, 1

In this section we start introducing one of the most fundamental concepts of modern mathematics: the notion of factor (or quotient) structure. We actually start with no structure at all, since in this section we only consider sets, but we will soon be looking at more and more structures when we consider factor groups or factor rings later on. We start with the following:

Definition 1.5.1 *If M is a set, a subset $\mathcal{R}$ of the cartesian product $M \times M$ is called a* (binary) relation *on M. We will write $x\mathcal{R}y$ if $(x,y) \in \mathcal{R}$, and we say that x is in the relation $\mathcal{R}$ with y.*

Definition 1.5.2 *A relation $\mathcal{E}$ on the set M is called an* equivalence relation *if it satisfies the following three properties for arbitrarily chosen $x, y, z \in M$:*
i) $x\mathcal{E}x$ (reflexivity).
ii) $x\mathcal{E}y \Rightarrow y\mathcal{E}x$ (symmetry).
iii) $x\mathcal{E}y$ and $y\mathcal{E}z \Rightarrow x\mathcal{E}z$ (transitivity).

Example 1.5.3 *The following relations are equivalence relations:*
i) On the set $\mathbb{Z}$: $a \equiv b \Leftrightarrow a = b$.
ii) On the set $\mathbb{Z}$: fix $n > 0$; then $a \equiv b\ (mod\ n) \Leftrightarrow n \mid a - b$. (This is called congruence modulo n.)
iii) On the set $\mathbb{Z}$: $a \sim_d b \Leftrightarrow a \mid b$ and $b \mid a$. (This is called association in divisibility.)
iv) On the set of points in the plane: fix a point C; then $A\mathcal{R}B \Leftrightarrow A$ and B are at the same distance from C.
v) Let M and N be sets and $f : M \longrightarrow N$ a function. Define the following relation on M: $x\mathcal{R}_f y \Leftrightarrow f(x) = f(y)$.

Definition 1.5.4 *Let $\mathcal{E}$ be an equivalence relation on the set M, and $x \in M$. We define the* equivalence class *of x relative to $\mathcal{E}$, by*

$$\hat{x}_{\mathcal{E}} = \{y \in M \mid x\mathcal{E}y\}.$$

If there is no danger of confusion we will omit the index and write $\hat{x} = \hat{x}_{\mathcal{E}}$. An equivalence class for $\mathcal{E}$ is the equivalence class of some element in M.

Example 1.5.5 *We describe the equivalence classes of the equivalence relations in Example 1.5.3:*
i) If $a \in \mathbb{Z}$, then $\hat{a} = \{a\}$.
ii) If $a \in \mathbb{Z}$, then $\hat{a} = \{a + kn \mid k \in \mathbb{Z}\}$.
iii) If $a \in \mathbb{Z}$, then $\hat{a} = \{a, -a\}$.
iv) $\hat{A}$=circle with center C and radius $|AB|$.
v) If $x \in M$, then $\hat{x} = f^{-1}(f(x)) = f^{-1}(\{f(x)\})$.

Remark 1.5.6 *If $y \in \hat{x}$, then $\hat{x} = \hat{y}$. Indeed, if $y \in \hat{x}$, then $\hat{y} \subseteq \hat{x}$, by symmetry and transitivity. Also, $x \in \hat{y}$ by symmetry, so $\hat{x} = \hat{y}$.*

We now recall the definition of a partition of a set.

Definition 1.5.7 *Let M be a set. A family $\{M_i\}_{i \in I}$ of subsets of M is called a* partition *of M if the following conditions are satisfied:*
i) $M_i \neq \emptyset$ for all $i \in I$.
ii) The sets in the family are disjoint, i.e. $M_i \cap M_j = \emptyset$ if $i, j \in I$, $i \neq j$.
iii) The sets cover M, i.e. $M = \cup_{i \in I} M_i$ (This means that any element in M belongs to one of the M_i's).

Proposition 1.5.8 *The equivalence classes of an equivalence relation $\mathcal{E}$ on the set M form a partition of M.*

Proof: We need to check the three conditions in Definition 1.5.7.
i) An equivalence class is $\hat{x}$ for some $x \in M$, so $\hat{x} \neq \emptyset$ because $x \in \hat{x}$ by reflexivity.
ii) Two equivalence classes are either disjoint or they coincide. Indeed, if $\hat{x} \cap \hat{y} \neq \emptyset$, let $z \in \hat{x} \cap \hat{y}$, and then $\hat{x} = \hat{y} = \hat{z}$ by Exercise 1.5.6.
iii) If $x \in M$, then $x \in \hat{x}$ as remarked in i). ∎

Example 1.5.9 *Let M be a set, and $\{M_i\}_{i \in I}$ a partition of M. Define the following relation on M: $x\mathcal{R}y \Leftrightarrow$ there exists $i \in I$ such that $x, y \in M_i$. Then $\mathcal{R}$ is an equivalence relation. To see this, note that the reflexive property follows from the fact that any $x \in M$ belongs to one of the M_i's. Symmetry is clear, because the order of x and y in "$x, y \in M_i$" is not important. Now, if $x, y \in M_i$ and $y, z \in M_j$, then $y \in M_i \cap M_j$, so $i = j$.*

Proposition 1.5.10 *There exists a bijective correspondence between the set of equivalence classes on a set M and the set of partitions on M.*

Proof: We start with and equivalence relation $\mathcal{E}$ on M. We form the partition of M consisting of the equivalence classes of $\mathcal{E}$, then we associate the equivalence relation $\mathcal{R}$ as in Example 1.5.9. This means that $x\mathcal{R}y$ if and only if x, y belong to an equivalence class of $\mathcal{E}$, if and only if $x\mathcal{E}y$, so $\mathcal{R} = \mathcal{E}$ and we got back to $\mathcal{E}$.
Conversely, start with a partition $\{M_i\}_{i \in I}$ of M, and consider the equivalence relation $\mathcal{R}$ as in Example 1.5.9. Then the equivalence classes of $\mathcal{R}$ are the M_i's, since we can check that if $x \in M_i$, then $M_i = \hat{x}$. ∎

Definition 1.5.11 *If M is a set and $\mathcal{E}$ is an equivalence relation on M, the* factor set *(or* quotient set*) of M through $\mathcal{E}$ is the set of equivalence classes of $\mathcal{E}$ and is denoted by $M/\mathcal{E}$. If we select one element in each equivalence* *class and denote the set of all these elements by $\mathcal{S}$, then the factor set of M through $\mathcal{E}$ can be described as*

$$M/\mathcal{E} = \{\hat{x} \mid x \in \mathcal{S}\}.$$

$\mathcal{S}$ is called a complete system of representatives *for the equivalence classes of $\mathcal{E}$,*

Example 1.5.12 *We describe the factor sets in Exercise 1.5.3 and indicate a complete system of representatives for each one:*
i) The integers form a complete system of representatives, so the factor set is in a bijective correspondence with $\mathbb{Z}$.
ii) A complete system of representatives is the set of all positive remainders: $\{0, 1, \ldots, n-1\}$, so the factor set can be described as $\mathbb{Z}_n = \{\hat{0}, \hat{1}, \ldots, \widehat{n-1}\}$ (We call $\mathbb{Z}_n$ "$\mathbb{Z}$ mod n", and if the context is clear, we can omit the hats). Indeed, for any $a \in \mathbb{Z}$ there exist q and r such that $a = nq+r$, $0 \leq r \leq n-1$ so $a \in \hat{r}$. Now, if $a \in \hat{i} \cap \hat{j}$, where $0 \leq i < j \leq n-1$, it follows that $n \mid j-i$, and since $0 \leq j-i \leq n-1$ it follows that $j-i = 0$, or $i = j$.
iii) The factor set is $\{\hat{n} \mid n \in \mathbb{Z}, \hat{n} = \{-n, n\}\ \}$. A complete system of representatives is $\mathbb{N}$.
iv) The factor set is the set of all circles centered at C. A complete system of representatives is a ray (half line) starting at C.
v) The factor set is the set of all fibers of f (i.e. preimages of images of elements of M). A complete set of representatives is $Im(f) = f(M)$.

1.6 Lecture 1.6: Equivalence relations, 2

We describe now the factor set in a way that does not make any reference to elements. We first give a second definition of a factor set, then show that the two definitions are equivalent.

Definition 1.6.1 *If M is a set, a factor set of M is a pair (N, p), where N is a set and $p : M \longrightarrow N$ is a surjective function.*

Example 1.6.2 *A factor set in the sense of Definition 1.5.11 is also a factor set in the sense of Definition 1.6.1, because the function $p : M \longrightarrow M/\mathcal{E}$, defined by $p(x) = \hat{x}$, is surjective (this function is called the canonical surjection).*

The following important result ensures that the two definitions of a factor set are actually the same:

Theorem 1.6.3 (The Universal Property of the Factor Set) *Let (N, p) be a factor set of the set M, let X be a set and $f : M \longrightarrow X$ a function.*
i) There exists a function $u : N \longrightarrow X$ such that $f = up$ (we say that f factors through p), which means that the diagram

$$\begin{tikzcd}
M \arrow[r, "p"] \arrow[dr, "f"'] & N \arrow[d, "u"] \\
& X
\end{tikzcd}$$

is commutative, if and only if $\mathcal{R}_p \subseteq \mathcal{R}_f$ (i.e. $p(x_1) = p(x_2) \Rightarrow f(x_1) = f(x_2)$). If u exists, then it is unique.
If u as in i) exists, then:
ii) u is surjective if and only if f is surjective.
iii) u is injective if and only if $\mathcal{R}_p = \mathcal{R}_f$ (i.e. $p(x_1) = p(x_2) \Leftrightarrow f(x_1) = f(x_2)$).

Proof: i) Assume that a function u like in the statement exists, and let $x_1, x_2 \in M$ such that $p(x_1) = p(x_2)$. Then $f(x_1) = u(p(x_1)) = u(p(x_2) = f(x_2)$. Conversely, assume that $p(x_1) = p(x_2) \Rightarrow f(x_1) = f(x_2)$ and let $y \in N$. Since p is surjective, let $x \in M$ such that $p(x) = y$, and define $u(y) = f(x)$. We need to show that the definition is correct, i.e. it does not depend on the choice of x. Indeed, if we have another $x_1 \in M$ such

that $p(x_1) = y$, then $p(x) = p(x_1) = y$, so $f(x) = f(x_1)$, and the definition of $u(y)$ does not depend on x. Now if two functions u_1 and u_2 with the property that $u_1 p = u_2 p = f$ exist, we let $y \in N$. Again since p is surjective there exists $x \in M$ such that $p(x) = y$, and hence $u_1(y) = u_1(p(x)) = f(x) = u_2(p(x)) = u_2(y)$, so $u_1 = u_2$.
ii) If u is surjective, then $f = up$ is surjective because it is a composition of surjective functions (see Proposition 1.2.8). Conversely, if $f = up$ is surjective, then u is surjective by Proposition 1.2.10.
iii) If u is injective, let $f(x_1) = f(x_2)$. It follows that $u(p(x_1)) = u(p(x_2))$, and so $p(x_1) = p(x_2)$. Conversely, assume that $p(x_1) = p(x_2) \Leftrightarrow f(x_1) = f(x_2)$ and let $y_1, y_2 \in N$ such that $u(y_1) = u(y_2)$. Since p is surjective let $x_1, x_2 \in M$ such that $p(x_1) = y_1$ and $p(x_2) = y_2$. Then we have $f(x_1) = u(p(x_1)) = u(p(x_2)) = f(x_2)$. By the hypothesis we have that $p(x_1) = p(x_2)$, so $y_1 = y_2$ and u is injective. ∎

Corollary 1.6.4 *If (N_1, p_1) and (N_2, p_2) are two factor sets of M such that $\mathcal{R}_{p_1} = \mathcal{R}_{p_2}$, then there exists a bijective function $u : N_1 \longrightarrow N_2$ such that $up_1 = p_2$.*

Proof: Take $(N, p) = (N_1, p_1)$, $X = N_2$ and $f = p_2$ in Theorem 1.6.3, hence we find u as in the statement, which is bijective. We can actually only use i) in Theorem 1.6.3: also take $(N, p) = (N_2, p_2)$, $X = N_1$ and $f = p_1$, and find v, $vp_2 = p_1$. Then $uvp_1 = p_1$, and $vup_2 = p_2$, so $uv = Id_{N_1}$ and $vu = Id_{N_2}$ by uniqueness. ∎

Corollary 1.6.5 *If (N, p) is a factor set of M, then there exists a bijection $u : N \longrightarrow M/\mathcal{R}_p$ such that $u \circ p$ is the canonical surjection sending an element to its equivalence class.*

Proof: Take $(N_1, p_1) = (N, p)$ and $(N_2, p_2) = (M/\mathcal{R}_p, can)$, where $can : M \longrightarrow M/\mathcal{R}_p$, $can(x) = \hat{x}$. Then $can(x_1) = can(x_2)$ if and only if $x_1 \mathcal{R}_p x_2$ if and only if $p(x_1) = p(x_2)$, and we can apply Corollary 1.6.4. ∎

1.7 Lecture 1.7: Equivalence relations, 3

In this lecture we count the equivalence relations on a finite set, then give some examples to help understanding the universal property of factor sets.

Remark 1.7.1 *We can use Proposition 1.2.12 to count equivalence relations on the set $M = \{x_1, x_2, \ldots, x_m\}$. If $k \leq m$, the number of equivalence relations on M such that the factor set has k elements is:*

$$E_{m,k} = \frac{1}{k!}(k^m - \binom{k}{1}(k-1)^{m-1} + \binom{k}{2}(k-2)^{m-2} + \ldots + (-1)^{k-1}\binom{k}{k-1}),$$

and so the number of equivalence relations on M is $E_{m,1}+E_{m,2}+\ldots+E_{m,m}$. Indeed, by Proposition 1.5.10 we need to count the partitions of M into k subsets. Each partition defines a surjection from M to the set $\{1, 2, \ldots, k\}$, defined by ordering the sets in the partition and sending each element of M to the index of the set in the partition that contains it. Since ordering the sets in the partition can be done in $k!$ different ways, it follows that the number of partitions of M into k subsets is the number of surjective functions from M to $\{1, 2, \ldots, k\}$ divided by $k!$.

Trying to solve the exercises below without looking at the solutions will help you better understand the concept of factor set and the universal property.

Exercise 1.7.2 *i) Let A be a set and $B \in \mathcal{P}(A)$. Define the following relation on $\mathcal{P}(A)$: if $X, Y \in \mathcal{P}(A)$, then $X\mathcal{R}Y$ if and only if $X \cap B = Y \cap B$. Show that $\mathcal{R}$ is an equivalence relation and there exists a bijection between the factor set $\mathcal{P}(A)/\mathcal{R}$ and $\mathcal{P}(B)$.*
ii) Let A and B be nonempty sets, and denote by B^A the set of functions from A to B. Choose $a \in A$, and define the following relation on B^A: $f\mathcal{R}g$ if and only if $f(a) = g(a)$. Show that $\mathcal{R}$ is an equivalence relation and there exists a bijection between the factor set $B^A/\mathcal{R}$ and B.
iii) With the same notation as in ii), let $C \in \mathcal{P}(A)$, and define the following relation on B^A: $f\mathcal{R}'g$ if and only if $f(x) = g(x)$ for all $x \in C$. Show that $\mathcal{R}'$ is an equivalence relation and there exists a bijection between the factor set $B^A/\mathcal{R}'$ and B^C.
iv) Show that i) and ii) can be obtained as particular cases of iii).

Solution: i) Let $f : \mathcal{P}(A) \longrightarrow \mathcal{P}(B)$, $f(X) = X \cap B$. Then f is surjective, $\mathcal{R} = \mathcal{R}_f$ is an equivalence relation by Exercise 1.5.3, v), and we can use Corollary 1.6.4 for $M = \mathcal{P}(A)$, $N_1 = \mathcal{P}(A)/\mathcal{R}$, $p_1 = can$, $N_2 = \mathcal{P}(B)$, $p_2 = f$.
ii) Let $F : B^A \longrightarrow B$, $F(f) = f(a)$. Then F is surjective, $\mathcal{R} = \mathcal{R}_F$ is an

equivalence relation by Exercise 1.5.3, v), and we can use Corollary 1.6.4 for $M = B^A$, $N_1 = B^A/\mathcal{R}$, $p_1 = can$, $N_2 = B$, $p_2 = F$.
iii) Let $F : B^A \longrightarrow B^C$, $F(f) =$ the restriction of f to C. Then F is surjective, $\mathcal{R} = \mathcal{R}_F$ is an equivalence relation by Exercise 1.5.3, v), and we can use Corollary 1.6.4 for $M = B^A$, $N_1 = B^A/\mathcal{R}$, $p_1 = can$, $N_2 = B^C$, $p_2 = F$.
iv) We can get ii) from iii) by taking $C = \{a\}$, and i) from iii) by taking $B = \{0, 1\}$, $A = A$ and $B = C$, and using the bijection between subsets and characteristic functions defined in the solution of Proposition 1.2.12, iii).

Exercise 1.7.3 *Show that the relation defined on $\mathbb{R}$ by $x\mathcal{R}y$ if and only if $x - y \in \mathbb{Z}$ is an equivalence relation, and there is a bijection between the factor set and a circle.*

Solution: Let C denote the unit circle centered at the origin, and define $f : \mathbb{R} \longrightarrow C$ by $f(x) = (\cos(2\pi(x - [x])), \sin(2\pi(x - [x])))$, where $[x]$ is the greatest integer less than or equal to x. Then $0 \leq x - [x] < 1$, and so $(x - [x]) - (y - [y]) \in \mathbb{Z}$ if and only if $(x - [x]) - (y - [y]) = 0$, i.e. $x - y \in \mathbb{Z}$, thus $\mathcal{R} = \mathcal{R}_f$, and we can use Corollary 1.6.4 for $M = \mathbb{R}$, $N_1 = \mathbb{R}/\mathcal{R}$, $p_1 = can$, $N_2 = C$, $p_2 = f$.

Chapter 2

Part II

2.1 Lecture 2.1: Groups, 1

Definition 2.1.1 *A* binary operation *on the set M is a function $\cdot : M \times M \longrightarrow M$, $\cdot(x, y) = xy$.*

Definition 2.1.2 *A set G, together with a binary operation $\cdot$ on G, denoted by $(G, \cdot)$, is called a* group *if the following conditions are satisfied:*
G1) the operation is associative, i.e. $x(yz) = (xy)z$ for all $x, y, z \in G$.
G2) the operation has an identity element, i.e. there exists an element $e \in G$ such that $ex = xe = x$ for all $x \in G$.
G3) every element in G has a symmetric element, i.e. for any $x \in G$ there exists an element $x' \in G$ such that $xx' = x'x = e$.
If the following condition is also satisfied:
G4) the operation is commutative, i.e. $xy = yx$ for all $x, y \in G$,
then the group is said to be abelian *(or* commutative*).*

As we can see in the above definition, our notation for a generic group operation will be multiplicative, i.e. a generic group will be denoted by $(G, \cdot)$, (or simply G if it is clear what the operation is) where the operation $\cdot : G \times G \longrightarrow G$, $\cdot(a, b) = ab$ is not necessarily the multiplication.

Remark 2.1.3 *Rewriting Definition 2.1.2 in additive notation, i.e. for $(G, +)$, where $+ : G \times G \longrightarrow G$, $+(x, y) = x + y$, produces the following:*
G1) $x + (y + z) = (x + y) + z$ for all $x, y, z \in G$.
G2) there exists an element $e \in G$ such that $e + x = x + e = x$ for all $x \in G$.
G3) for any $x \in G$ there exists an element $x' \in G$ such that $x + x' = x' + x = e$.

G is abelian if the following condition is also satisfied:
G4) $x + y = y + x$ for all $x, y \in G$.

Proposition 2.1.4 *i) If e_1 and e_2 are identity elements in a group, i.e. they both satisfy condition G2) in Definition 2.1.2, then prove that $e_1 = e_2$. This means that the identity element in a group is unique. Our notation for it will be 1_G if the notation for the operation of the group is multiplicative, and 0_G if the notation for the operation of the group is additive.*
ii) Show that the symmetric element of an element x in a group G is unique, i.e. if x' and x'' both satisfy the condition in Definition 2.1.2, G3), then $x' = x''$. If the notation is multiplicative, we will call the symmetric element of x the inverse *of x and we will denote it by x^{-1}. If the notation is additive, we will call the symmetric element of x* the opposite *of x and we will denote it by $-x$.*
iii) Prove that if in a group G we have $xy = xz$, it follows that $y = z$ (this is called the cancelation law).

Proof: i) Taking $x = e_2$ in G2) for e_1 we get: $e_1e_2 = e_2e_1 = e_2$. Taking $x = e_1$ in G2) for e_2 we get: $e_2e_1 = e_1e_2 = e_1$. Comparing the two we get $e_1e_2 = e_2e_1 = e_2 = e_1$.
ii) Since $xx' = 1_G$, it follows that $x''xx' = x''$, and since $x''x = 1_G$, we get that $x' = x''$.
iii) If $xy = xz$, then $x^{-1}xy = x^{-1}xz$, so $y = z$. ∎

Example 2.1.5 *i) The number sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are all groups under addition, but they are not groups under multiplication (why?).*
ii) $(S(M), \circ)$ is a group, called the symmetric group on the set M,

$$S(M) = \{f : M \longrightarrow M \mid f \text{ is bijective}\}$$

and $\circ$ is the composition of functions. The elements of $S(M)$ are called permutations. We will denote $S_n = S(\{1, 2, \ldots, n\})$.
The composition of two bijective functions is bijective; composition of functions is associative; the identity element is Id_M; a bijective function is invertible. $S(M)$ is not necessarily abelian: S_2 is abelian, but S_3 is not:
We will write

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

if $\sigma(1) = 2$, $\sigma(2) = 3$, and $\sigma(3) = 1$. We will also write this as $\sigma = (123)$ (the cycle *$(a_1a_2 \ldots a_k)$ in S_n is the function that sends a_i to a_{i+1} for $i = 1, \ldots, k-1$, and a_k to a_1, and leaves all the other elements unchanged; the set $\{a_1, a_2, \ldots, a_k\}$ is called the* orbit *of the cycle, and k is called its length). With this notation we have*

$$S_3 = \{Id, (12), (13), (23), (123), (132)\}.$$

Each of $Id, (12), (13), (23)$ *is its own inverse, and the inverse of* (123) *is* (132). *Note that* S_3 *is not abelian because* $(12)(13) = (132)$ *and* $(13)(12) = (123)$.

iii) $(GL_2(\mathbb{C}), \cdot)$ *is a nonabelian group, where*

$$GL_2(\mathbb{C}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{C}, ad - bc \neq 0 \right\}$$

and $\cdot$ *is the multiplication of matrices. Recall that multiplication of matrices is defined as*

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} = \begin{bmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{bmatrix}$$

and it is associative. The identity element is

$$I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

and the inverse of a matrix is given by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}.$$

$GL_2(\mathbb{C})$ *is nonabelian because*

$$\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}$$

and

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix}.$$

iv) $(Q_8, \cdot)$ *is a nonabelian group, where* $\cdot$ *is the multiplication of matrices, and* Q_8 *is the following subset of* $M_2(\mathbb{C})$:

$$Q_8 = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix}, \right.$$
$$\left. \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix} \right\}.$$

The elements of Q_8 *are called quaternions. If we denote*

$$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad -1 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \quad i = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \quad -i = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

$$j = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \quad -j = \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix} \quad k = \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix} \quad -k = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$$

then we can check that $i^2 = j^2 = k^2 = ijk = -1$, *and we can use these relations to check that* $\cdot$ *is an operation on* Q_8. Q_8 *is not abelian because* $ij \neq ji$.
v) $(\mathcal{P}(M), *)$, *is an abelian group, where* M *is a set, and* $A * B = \{x \in M \mid x \in A \cup B, x \notin A \cap B\}$. *If* $A, B, C \in \mathcal{P}(M)$, *then both* $A * (B * C)$ *and* $(A * B) * C$ *are equal to the set*

$$\{x \in M \mid x \in A \cup B \cup C, x \notin (A \cap B) \cup (A \cap C) \cup (B \cap C)\},$$

so $*$ *is associative. The identity element is* $\emptyset$ *and the symmetric of the set* A *is* A *itself.*

2.2 Lecture 2.2: Groups, 2

We are now going to define two operations on the set $\mathbb{Z}_n$ (see Example 1.5.12, ii)). In order to do that we will need the following:

Proposition 2.2.1 *Let $n > 0$ be an integer, and assume that $a \equiv b \ (mod\, n)$ and $c \equiv d \ (mod\, n)$. Then:*
i) $a + c \equiv b + d \ (mod\, n)$.
ii) $ac \equiv bd \ (mod\, n)$.

Proof: i) Since $n \mid a-b$ and $n \mid c-d$, let k, l be integers such that $a-b = kn$ and $c-d = ln$. Then $a - b + c - d = (k+l)n$, so $n \mid a + c - (b+d)$.
ii) With the notation of i), we have $ac - bd = ac - bc + bc - bd = c(a-b) + b(c-d) = ckn + bln = n(ck + bl)$, so $n \mid ac - bd$. ∎

The previous exercise shows that we can talk about the sum and product of elements in $\mathbb{Z}_n$: if $\hat{a}, \hat{b} \in \mathbb{Z}_n$, define

$$\hat{a} + \hat{b} = \widehat{a+b},$$

and

$$\hat{a}\hat{b} = \widehat{ab}.$$

Exercise 2.2.2 *Which of the following sets are groups:*
i) $(\mathbb{Z}_n, +)$.
ii) $(\mathbb{Z}_n, \cdot)$.
iii) $(\mathbf{U}_n, \cdot)$, where $\mathbf{U}_n = \{\hat{a} \in \mathbb{Z}_n \mid 1 = (a, n)\}$.
iv) $(\mathbf{U}_n, +)$.

Solution: i) $(\mathbb{Z}_n, +)$ is an abelian group. By Exercise 2.2.1 we have that $+$ is an operation, and it is associative and commutative because addition of the integers is so. The identity element is $\hat{0}$, and the opposite of $\hat{a}$ is $\widehat{n-a}$.
ii) $(\mathbb{Z}_n, \cdot)$ is not a group if $n \neq 1$, because G3) is not satisfied, $\hat{0} \cdot \hat{a} = \hat{0} \neq \hat{1}$ for all a.
iii) $(\mathbf{U}_n, \cdot)$ is an abelian group, because $\cdot$ is associative and commutative, and $\hat{1}$ is the identity element. If $1 = (a, n)$, then $1 = au + nv$, so $\hat{1} = \widehat{au + nv} = \hat{a}\hat{u} + \hat{n}\hat{v} = \hat{a}\hat{u}$, so the inverse of $\hat{a}$ is $\hat{u}$.
iv) We clearly have that $\hat{1} \in \mathbf{U}_n$, but if we add n copies of $\hat{1}$ we get $\hat{0} \notin \mathbf{U}_n$, so $+$ is not an operation on $\mathbf{U}_n$.

Exercise 2.2.3 *Let G_1 and G_2 be groups, and define the following operation on the cartesian product $G_1 \times G_2$: $(x, y) \cdot (x', y') = (xx', yy')$, where $x, x' \in G_1$ and $y, y' \in G_2$. Show that $G_1 \times G_2$ is a group with this operation (it is called the* direct product *of the groups G_1 and G_2).*

Definition 2.2.4 *If G and G' are groups, a function $f : G \longrightarrow G'$ is called a* group morphism (or homomorphism) *if f preserves the group operation, i.e. $f(xy) = f(x)f(y)$ for all $x, y \in G$. The morphism f is said to be an injective morphism if the function f is injective. Similarly, if the function f is surjective, we say that f is a surjective morphism. A group morphism $f : G \longrightarrow G'$ is called an* isomorphism *if there exists a group morphism $f' : G' \longrightarrow G$ such that $f \circ f' = Id_{G'}$ and $f' \circ f = Id_G$; we then say that the groups G and G' are* isomorphic, *and we write $G \simeq G'$. A morphism from G to G is called an* endomorphism *of G, and an isomorphism from G to G is called an* automorphism *of G.*

The following result lists properties of group morphisms:

Proposition 2.2.5 *Let $f : G \longrightarrow G'$ and $g : G' \longrightarrow G''$ be group morphisms. Then:*
i) $f(1_G) = 1_{G'}$.
ii) For $x \in G$, we have $f(x^{-1}) = f(x)^{-1}$.
iii) gf is a group morphism.
iv) f is an isomorphism if and only if f is bijective.

Proof: i) $1_G \cdot 1_G = 1_G$, so $f(1_G \cdot 1_G) = f(1_G)$, or $f(1_G)f(1_G) = f(1_G) = f(1_G)1_{G'}$, and the assertion follows from the cancelation law.
ii) We have that $f(x)f(x^{-1}) = f(xx^{-1}) = f(1_G) = 1_{G'}$, so the assertion follows by multiplying both sides of this equality by $f(x)^{-1}$.
iii) $gf(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y))$.
iv) We have to prove that if the morphism f is bijective, then its inverse f^{-1} is also a morphism. We have $f^{-1}(x'y') = f^{-1}(f(f^{-1}(x'))f(f^{-1}(y'))) = f^{-1}(f(f^{-1}(x')f^{-1}(y'))) = f^{-1}f(f^{-1}(x')f^{-1}(y')) = f^{-1}(x')f^{-1}(y')$. ∎

Exercise 2.2.6 *Which of the following maps are group morphisms? For each of them decide if they are injective, surjective, or an isomorphism. If a morphism is an isomorphism, find the inverse.*
i) $Id_G : G \longrightarrow G$.
ii) $i : \mathbb{Z} \longrightarrow \mathbb{Q}$, $i(x) = x/1$ for $x \in \mathbb{Z}$.
iii) If $x \in G$, $f_x : G \longrightarrow G$, $f_x(g) = xgx^{-1}$ for all $g \in G$.
iv) $\ln : (0, \infty) \longrightarrow \mathbb{R}$.
v) $f : \mathbb{Z}_4 \longrightarrow \mathbb{Z}_2$, $f(\hat{a}(mod\, 4)) = \hat{a}(mod\, 2)$.
vi) $g : \mathbb{Z}_2 \longrightarrow \mathbb{Z}_4$, $g(\hat{a}(mod\, 2)) = \hat{a}(mod\, 4)$.
vii) $p_1 : G_1 \times G_2 \longrightarrow G_1$, $p_1(x, y) = x$.

Solution: i) it is an isomorphism, and it is its own inverse.
ii) this is an injective morphism.
iii) $f_x(gh) = xghx^{-1} = xgx^{-1}xhx^{-1} = f_x(g)f_x(h)$. It is an isomorphism, and the inverse of f_x is $f_{x^{-1}}$.

iv) First, make sure you understand what the group operations are. Next, we have $\ln(xy) = \ln(x) + \ln(y)$, so ln is a group morphism. Since ln is bijective, with inverse the exponential function, ln is an isomorphism.
v) Let us check that f is correctly defined: if $\hat{a}(mod\ 4) = \hat{b}(mod\ 4)$, then $4 \mid a - b$, so $2 \mid a - b$ and hence $\hat{a}(mod\ 2) = \hat{b}(mod\ 2)$, or $f(\hat{a}(mod\ 4)) = f(\hat{b}(mod\ 4))$, and f is correctly defined. By the definition of addition mod 4 or mod 2, f is a group morphism which is clearly surjective.
vi) g is not correctly defined: $\hat{1}(mod\ 2) = \hat{3}(mod\ 2)$, but $\hat{1}(mod\ 4) \neq \hat{3}(mod\ 4))$.
vii) We have $p_1((x, y)(x'y')) = p_1(xx', yy') = xx' = p_1(x, y)p_1(x', y')$, so p_1 is a group morphism. It is clearly surjective, because if $x \in G_1$, then $x = p_1(x, 1_{G_2})$.

Exercise 2.2.7 *If $\varphi : M \longrightarrow N$ is a bijection, show that $S(M) \simeq S(N)$ (see Exercise 2.1.5, xviii)). In particular, if M has n elements, then $M \simeq S_n$.*

Solution: Define $\psi : S(M) \longrightarrow S(N)$ by $\psi(f) = \varphi f \varphi^{-1}$ for $f \in S(M)$. It is easy to check that ψ is a morphism and that its inverse is $\psi^{-1} : S(N) \longrightarrow S(M)$, $\psi^{-1}(g) = \varphi^{-1} g \varphi$.

Definition 2.2.8 *If G is a group and $a \in G$. If all powers of a are distinct we say that a has infinite order and we write $|a| = \infty$. If there exists a power of a that is equal to 1, we call the smallest such power the order of a and we denote it by $|a|$. Using the division algorithm we see that if $a^n = 1$, then we write $n = q\,|a| + r$, where $0 \leq r < |a|$, and we have $1 = a^{q|a|}a^r = a^r$, so $r = 0$, and therefore $|a| \mid n$.*

The oder of $1 \in \mathbb{Z}$ is infinite. The following exercise gives examples of elements of finite order.

Exercise 2.2.9 *Find the orders of all the elements of the group:*
i) $\mathbb{Z}_4$.
ii) $\mathbb{Z}_2 \times \mathbb{Z}_2$.
iii) $\mathbb{Z}_6$.
iv) S_3.
v) The quaternion group Q_8.

Solution: The order of the identity element in a group is 1, so we will ignore the identity element in all cases.
i) The order of 1 and 3 is 4, and the order of 2 is 2.
ii) All elements different from $(0, 0)$ have order 2.
iii) The order of 1 and 5 is 6, the order of 2 and 4 is 3, and the order of 3 is 2.

iv) The order of $(12), (13)$, and (23) is 2, and the order of (123) and (132) is 3.
v) The order of -1 is 2, and the order of $i, -i, j, -j, k$, and $-k$ is 4.

The group of transformations of a regular polygon with n sides, which is called the dihedral group D_n, is obtained as follows: we denote by θ the counterclockwise rotation of $\frac{2\pi}{n}$ about the center of the polygon, and by τ the flip along one of the perpendiculars from the center to one of the sides, then we can check that

$$D_n = \{1, \theta, \theta^2, \ldots, \theta^{n-1}, \tau, \theta\tau, \theta^2\tau, \ldots, \theta^{n-1}\tau\},$$

$\theta^n = \tau^2 = 1$, $\tau\theta = \theta^{n-1}\tau$.

2.3 Lecture 2.3: Subgroups, 1

We know that both $(\mathbb{R}^*, \cdot)$ and $((0,\infty), \cdot)$ are groups. This means that the operation of the group $(\mathbb{R}^*, \cdot)$ restricted to the subset $(0,\infty)$ is also an operation, and it satisfies the axioms in the definition of a group. We say that the operation of the group $(\mathbb{R}^*, \cdot)$ induces a group structure on the subset $(0,\infty)$, or that $(0,\infty)$ is a subgroup of $\mathbb{R}^*$. In general we have the following:

Definition 2.3.1 *Let G be a group, and H a nonempty subset of G. Then H is called a* subgroup *of G if the operation on G induces an operation on H such that H together with the induced operation forms a group. If H is a subgroup of G we write $H \leq G$.*

Trivial examples of subgroups in any group G are the so called improper subgroups $\{1_G\}$ and G itself. When checking that a certain nonempty subset H of a group G is a subgroup we need to check three conditions:
SG1) If $x, y \in H$, then $xy \in H$. This means that the operation on G induces an operation on H. (If this is true, we say that H is closed, or stable, under the operation of G.)
Associativity is a gimme, because we know it holds for elements of G, and all elements of H are also elements of G.
SG2) $1_G \in H$. This comes from condition G2) in the definition of a group applied to H: if e is an identity element of H, then $ee = e$ in H, and when we consider this equality in G and multiply both sides by e^{-1} we get that $e = 1_G$.
SG3) If $x \in H$, then $x^{-1} \in H$. Because of $G2$, any inverse of x in H will be an inverse of x in G, so the assertion is true because of the uniqueness of the inverse.

Proposition 2.3.2 *Let G be a group and $\emptyset \neq H \subseteq G$. Then the following assertions are equivalent:*
i) $H \leq G$.
ii) If $x, y \in H$, then $x^{-1}y \in H$.

Proof: i) ⇒ ii). Let $x, y \in H$. By SG3) we have $x^{-1} \in H$, and by SG1) we get $x^{-1}y \in H$.
ii) ⇒ i). We first check SG2). Let $x \in H$, then by ii) $x^{-1}x = 1_G \in H$. Now for $x \in H$ we can use ii) for x and 1_G to get $x^{-1}1_G = x^{-1} \in H$, so SG3) also holds. Finally, if $x, y \in H$, then $xy = (x^{-1})^{-1}y \in H$ by SG3) and ii), so SG1) holds too. ∎

Exercise 2.3.3 *Write in additive notation conditions SG1), SG2), SG3), and Proposition 2.3.2.*

Exercise 2.3.4 *Let G be a group and $\emptyset \neq H \subseteq G$. Then the following assertions are equivalent:*
i) $H \leq G$.
ii) If $x, y \in H$, then $xy^{-1} \in H$.

If $\emptyset \neq H \subseteq G$ is a finite subset, it is a lot easier to check that $H \leq G$:

Proposition 2.3.5 *Let G be a group and $\emptyset \neq H \subseteq G$ a finite subset. Then the following assertions are equivalent:*
i) $H \leq G$.
ii) If $x, y \in H$, then $xy \in H$.

Proof: We only prove ii) ⇒ i), because the converse is obvious. Let $x \in H$, and consider the function $\varphi : H \longrightarrow H$, defined by $\varphi(y) = xy$ for $y \in H$. Then φ takes values in H because of ii), and it is injective because of the cancelation law in G. Since H is finite, it follows that φ is also surjective, so there exists $x' \in H$ such that $\varphi(x') = x$. This means $xx' = x$, and after considering this equality in G and multiplying both sides on the left by x^{-1}, we get that $x' = 1_G$, so we checked SG2). We now use again the fact that φ is surjective, so there exists $x'' \in H$ such that $\varphi(x'') = 1_G$. This means $xx'' = 1_G$, and after considering this equality in G and multiplying both sides on the left by x^{-1}, we get that $x'' = x^{-1}$, so we also checked SG3). ∎

Exercise 2.3.6 *Determine whether each of the following subsets is a subgroup:*
i) $\mathbb{Z} \subseteq \mathbb{Q}$.
ii) $\mathbb{N} \subseteq \mathbb{Z}$.
iii) If $n \in \mathbb{Z}$, $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\} \subseteq \mathbb{Z}$.
iv) $\{0, 2, 4\} \subseteq \mathbb{Z}_5$.
v) $\{0, 2, 4\} \subseteq \mathbb{Z}_6$.
vi) $\{Id, (12)\} \subseteq S_3$.
vii) $\{Id, (12), (13)\} \subseteq S_3$.
viii) $\{Id, (123)\} \subseteq S_3$.
ix) $\{Id, (123), (132)\} \subseteq S_3$.
x) $\{1, -1, i, -i\} \subseteq Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$, the quaternion group, see Exercise 2.1.5, xxvi).
xi) $H \cap K$, where $H, K \leq G$.
xii) $H \cup K$, where $H, K \leq G$.

Solution: i) $\mathbb{Z} \leq \mathbb{Q}$, because $0 \in \mathbb{Z}$, and $n - m \in \mathbb{Z}$ for all integers m, n.
ii) Not a subgroup, $1 - 2 \notin \mathbb{N}$.
iii) $n\mathbb{Z} \leq \mathbb{Z}$, because $0 = n \cdot 0 \in n\mathbb{Z}$, and if $k, k' \in \mathbb{Z}$, then

$$nk - nk' = n(k - k') \in n\mathbb{Z}.$$

iv) Not a subgroup, $2+4=1 \notin \{0,2,4\}$.
v) $\{0,2,4\} \leq \mathbb{Z}_6$, because $\{0,2,4\}$ is closed under $+$:

$$2+2=4, \;\; 2+4=0, \;\; 4+4=2.$$

vi) $\{Id,(12)\} \leq S_3$, because $(12)(12)=Id$.
vii) Not a subgroup, $(12)(13)=(132) \notin \{Id,(12),(13)\}$.
viii) Not a subgroup, $(123)(123)=(132) \notin \{Id,(123)\}$.
ix) $\{Id,(123),(132)\} \leq S_3$, because $(123)(123)=(132)$ and $(132)(132)=(123)$.
x) $\{1,-1,i,-i\} \leq Q_8$, because

$$x \in \{1,-1,i,-i\} \Rightarrow -x \in \{1,-1,i,-i\},$$

so we only have to check that $i^2=-1$.
xi) Clearly $H \cap K \neq \emptyset$, because $1_G \in H \cap K$. If $x,y \in H \cap K$, then $x,y \in H$ and $x,y \in K$, so $x^{-1}y \in H$ and $x^{-1}y \in K$, so $x^{-1}y \in H \cap K$. Note that the same proof works for the intersection of an arbitrary family of subgroups, not just two subgroups.
xii) If one of H or K is contained in the other one, then the union is equal to the larger of the two, and it is therefore a subgroup. Now if $H \not\subseteq K$ and $K \not\subseteq H$ we show that $H \cup K$ is not a subgroup. Indeed, let $x \in H$, $x \notin K$, $y \in K$, and $y \notin H$. Then $xy \notin H \cup K$, because if $xy \in H$ it follows that $y = x^{-1}xy \in H$, and if $xy \in K$, then $x = xyy^{-1} \in K$.

We now show that all the subgroups of $\mathbb{Z}$ look like the one in Exercise 2.3.6 iii).

Proposition 2.3.7 *If $H \leq \mathbb{Z}$, then there exists $n \in \mathbb{Z}$ such that $H = n\mathbb{Z}$.*

Proof: If $H=\{0\}$ we take $n=0$. If $H \neq \{0\}$, we consider the set $W=\{x \in H \mid x>0\}$. Then if $0 \neq x \in H$, then we also have $-x \in H$ and so $W \neq \emptyset$. By the well-ordering principle, W has a smallest element n. Since H is a subgroup and $n \in H$, it is clear that $n\mathbb{Z} \subseteq H$. Conversely, if $m \in H$, we write $m = qn + r$, where $0 \leq n$. Since $r = m - nq \in H$ it follows that $r=0$ because otherwise we get a contradiction with the fact that n is the least element in W, and so $m = nq \in n\mathbb{Z}$. ∎

Exercise 2.3.8 *Let $f: G \longrightarrow G'$ be a morphism of groups. Then:*
i) $f(G) \leq G'$ (we denote $f(G)$ by $Im(f)$ and call it the image of f).
ii) $f^{-1}(1_{G'}) \leq G$ (we denote $f^{-1}(1_{G'})$ by $Ker(f)$ and call it the kernel of f).
iii) If $H \leq G$, then $f(H) \leq G'$.
iv) If $H' \leq G'$, then $f^{-1}(H') \leq G$.
v) f is surjective $\Leftrightarrow Im(f) = G'$.
vi) f is injective $\Leftrightarrow Ker(f) = \{1_G\}$.

Solution: i) $1_{G'} = f(1_G) \in f(G)$, and if $x', y' \in f(G)$, then $x' = f(x)$ and $y' = f(y)$, so $x'^{-1}y' = f(x)^{-1}f(y) = f(x^{-1})f(y) = f(x^{-1}y) \in f(G)$.
ii) $1_G \in f^{-1}(1_{G'})$, and if $x, y \in f^{-1}(1_{G'})$, then $f(x^{-1}y) = f(x)^{-1}f(y) = 1_G$.
iii) $1_{G'} = f(1_G) \in f(H)$, and if $x', y' \in f(H)$, then $x' = f(x)$ and $y' = f(y)$ for some $x, y \in H$, so $x^{-1}y \in H$ and $x'^{-1}y' = f(x)^{-1}f(y) = f(x^{-1})f(y) = f(x^{-1}y) \in f(H)$.
iv) $1_G \in f^{-1}(H')$, and if $x, y \in f^{-1}(H')$, then $f(x), f(y) \in H'$, and $f(x^{-1}y) = f(x)^{-1}f(y) = H'$.
v) is obvious.
vi) Assume that f is injective, and let $x \in Ker(f)$. Then $f(x) = f(1_G) = 1_{G'}$, so $x = 1_G$. Conversely, we assume now that $Ker(f) = \{1_G\}$ and we prove that f is injective. Let $x, y \in G$ such that $f(x) = f(y)$. Then $f(x)f(y)^{-1} = 1_{G'}$, so $f(xy^{-1}) = 1_{G'}$, i.e. $xy^{-1} \in Ker(f) = \{1_G\}$. Therefore $xy^{-1} = 1_G$, so $x = y$.

2.4 Lecture 2.4: Subgroups, 2

Let G be a group, and E a subset of G. There exists a smallest subgroup of G that contains all the elements of E, it is the intersection of all the subgroups containing E. Such subgroups clearly exist, since G contains E. We call it the subgroup generated by the set E. It is clear that the subgroup generated by $\emptyset$ is $\{1_G\}$. If the group is generated by a set with one element, the group is called cyclic. A description of the subgroup generated by a set is given in the following:

Proposition 2.4.1 *Let E be a subset of the group G. The subgroup H generated by E consists of all finite products of elements of E or inverses of elements of E.*

Proof: Let H' the set of all finite products of elements of E or inverses of elements of E. Since H is a subgroup that contains E, it is clear that $H' \subseteq H$. Since H is the smallest subgroup that contains E, in order to prove the inclusion $H \subseteq H'$ it is enough to prove that H' is a subgroup that contains E. It is clear that H' contains E, and that if $x, y \in H'$, then $x^{-1}y \in H'$, which proves the claim. ▮

If $H, K \leq G$, the subgroup generated by $H \cup K$ will be denoted by HK (or $H + K$ in additive notation). By the previous result, if G is a cyclic group generated by the element a, then we have

$$G = \{a^k \mid k \in \mathbb{Z}\},$$

where

$$a^k = \begin{cases} \text{the product of } k \text{ copies of } a & \text{if } k > 0 \\ 1_G & \text{if } k = 0 \\ \text{the product of } -k \text{ copies of } a^{-1} & \text{if } k < 0 \end{cases}$$

In additive notation, if G is a cyclic group generated by the element a, then we have

$$G = \{ka \mid k \in \mathbb{Z}\},$$

where

$$ka = \begin{cases} \text{the sum of } k \text{ copies of } a & \text{if } k > 0 \\ 0_G & \text{if } k = 0 \\ \text{the sum of } -k \text{ copies of } -a & \text{if } k < 0 \end{cases}$$

Example 2.4.2 *It is clear that $\mathbb{Z}$ is cyclic (it is generated by 1 or -1), and $n\mathbb{Z}$ is also cyclic for any n (it is generated by n or $-n$). Then $\mathbb{Z}_n$ is cyclic, generated by 1. Since all cyclic groups are clearly abelian, S_3 is not cyclic. It can also be checked that $\mathbb{Z}_2 \times \mathbb{Z}_2$ is abelian but not cyclic.*

We now introduce an important class of subgroups.

Definition 2.4.3 *Let G be a group and $H \leq G$. We will say that H is a* normal *subgroup of G (and we will write $H \trianglelefteq G$) if for any $x \in G$ and $h \in H$ we have $xhx^{-1} \in H$.*

If we denote $xHx^{-1} = \{xhx^{-1} \mid h \in H\}$, the condition in the definition above becomes $xHx^{-1} \subseteq H$ for all $x \in G$ (we can also use $\leq$ instead of $\subseteq$, since xHx^{-1} is a subgroup of G, hence of H if it is contained in it). It is clear that the trivial subgroups $\{1_G\}$ and G are normal, and also that any subgroup of an abelian group is normal. Here are some examples and counterexamples.

Exercise 2.4.4 *Which of the following subsets are normal subgroups:*
i) $\mathbb{Z} \subseteq \mathbb{Q}$.
ii) If $n \in \mathbb{Z}$, $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\} \subseteq \mathbb{Z}$.
iii) $\{0, 2, 4\} \subseteq \mathbb{Z}_6$.
iv) $\{Id, (12)\} \subseteq S_3$.
v) $\{Id, (123), (132)\} \subseteq S_3$.
vi) $\{1, -1, i, -i\} \subseteq Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$*, the quaternion group.*

Solution: i), ii), iii). The subsets are subgroups of abelian groups by Exercise 2.3.6, so they are normal subgroups.
iv) No, because $(13)(12)(13) = (23) \notin \{Id, (12)\}$.
v) $\{Id, (123), (132)\} \trianglelefteq S_3$, because we can check that

$$(12)(123)(12) = (13)(123)(13) = (23)(123)(23) = (132)$$

and

$$(12)(132)(12) = (13)(132)(13) = (23)(132)(23) = (123).$$

vi) $\{1, -1, i, -i\} \trianglelefteq Q_8$. Since $x \in \{1, -1, i, -i\} \Rightarrow -x \in \{1, -1, i, -i\}$, we only need to check that $ii(-i) = i \in \{1, -1, i, -i\}$, $ji(-j) = -i \in \{1, -1, i, -i\}$, and $ki(-k) = -i \in \{1, -1, i, -i\}$, so $\{1, -1, i, -i\} \trianglelefteq Q_8$.

We end this section with the study of the behavior of normal groups through group morphisms.

Proposition 2.4.5 *Let $f : G \longrightarrow G'$ be a group morphism. Then the following assertions hold:*
i) If $H' \trianglelefteq G'$, then $f^{-1}(H') \trianglelefteq G$.
ii) If f is surjective and $H \trianglelefteq G$, then $f(H) \trianglelefteq G'$.

Proof: i) We know from Exercise 2.3.8 iv) that $f^{-1}(H') \leq G$. Let $x \in G$ and $h \in f^{-1}(H')$. We know that $f(h) \in H'$ and we want to

prove that $f(xhx^{-1}) \in H'$. We have $f(xhx^{-1}) = f(x)f(h)f(x^{-1}) = f(x)f(h)f(x)^{-1} \in H'$, because $H' \trianglelefteq G'$.
ii) We know from Exercise 2.3.8 iii) that $f(H) \leq G'$. Let $x' \in G'$ and $h' \in f(H)$. Then $h' = f(h)$ for some $h \in H$, and since f is surjective, $x' = f(x)$ for some $x \in G$. We then have $x'h'x'^{-1} = f(x)f(h)f(x)^{-1} = f(x)f(h)f(x^{-1}) = f(xhx^{-1}) \in f(H)$, since $H \trianglelefteq G$. ∎

Example 2.4.6 *The following example shows that the assertion in Proposition 2.4.5 ii) is not true if f is not surjective. Let $i : \{Id, (12)\} \longrightarrow S_3$ denote the inclusion. Then i is a group morphism because $\{Id, (12)\} \leq S_3$, $\{Id, (12)\} \trianglelefteq \{Id, (12)\}$, but $\{Id, (12)\}$ is not normal in S_3 by Exercise 2.4.4 iv).*

Corollary 2.4.7 *Let $f : G \longrightarrow G'$ be a surjective group morphism. There exists a bijective correspondence between the subgroups of G' and the subgroups of G which contain $Ker(f)$. This correspondence induces a bijective correspondence between the normal subgroups of G' and the normal subgroups of G which contain $Ker(f)$.*

Proof: Let $H' \leq G'$. Then $f^{-1}(H') \leq G$ and $Ker(f) = f^{-1}(1_G) \subseteq f^{-1}(H')$. If $H \leq G$ and $Ker(f) \subseteq H$, then $f(H) \leq G'$. We prove first that

$$f(f^{-1}(H')) = H' \tag{2.1}$$

Let $h' \in H'$. Since f is surjective, $h' = f(h)$ for some $h \in G$. Since it is clear that $h \in f^{-1}(H')$ this shows that $H' \subseteq f(f^{-1}(H'))$. Conversely, let $h' \in f(f^{-1}(H'))$. Then $h' = f(h)$, where $h \in f^{-1}(H')$. But this means $f(h) \in H'$, so $h' \in H'$.
We now prove

$$f^{-1}(f(H)) = H \tag{2.2}$$

Indeed, if $h \in f^{-1}(f(H))$, then $f(h) \in f(H)$, so $f(h) = f(h_1)$, where $h_1 \in H$. Then $hh_1^{-1} \in Ker(f) \subseteq H$, so $h \in H$. Conversely, if $h \in H$, then $f(h) \in f(H)$, and so clearly $h \in f^{-1}(f(H))$.
By (2.1) and (2.2) we see that the correspondences defined above are bijections inverse to each other. The statement about normal subgroups follows from Proposition 2.4.5. ∎

Corollary 2.4.8 *Show that any subgroup of $\mathbb{Z}_n$ is generated by an element $\hat{d}$, where $d \mid n$.*

Proof: The map $f : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ defined by $f(a) = \hat{a}$ is a surjective group morphism, so by Corollary 2.4.7 there exists a bijective correspondence between the subgroups of $\mathbb{Z}_n$ and the subgroups of $\mathbb{Z}$ that contain $Ker(f) = n\mathbb{Z}$. Now $a\mathbb{Z} \subseteq b\mathbb{Z} \Leftrightarrow a \in b\mathbb{Z} \Leftrightarrow b \mid a$. Therefore, a subgroup of $\mathbb{Z}_n$ is $f(d\mathbb{Z})$ for some $d \mid n$. ∎

2.5 Lecture 2.5: Factor groups

Let G be a group and $H \leq G$. We define two relations on G:

$$x \equiv_l y \; (mod\, H) \Longleftrightarrow x^{-1}y \in H,$$

and

$$x \equiv_r y \; (mod\, H) \Longleftrightarrow xy^{-1} \in H.$$

Proposition 2.5.1 *$\equiv_l$ $(mod\ H)$ and $\equiv_r$ $(mod\ H)$ are equivalence relations on G.*

Proof: We prove only one of them. If $x \in G$, then $x^{-1}x = 1_G \in H$, so the relation is reflexive. If $x^{-1}y \in H$, then $(x^{-1}y)^{-1} = y^{-1}x \in H$, so the relation is symmetric. Now if $x^{-1}y \in H$ and $y^{-1}z \in H$, then $x^{-1}z = x^{-1}yy^{-1}z \in H$, so the relation is transitive. ▮

Proposition 2.5.2 *Let G be a group, $H \leq G$ and $x \in G$. Denote by $\hat{x}$ the equivalence class of x with respect to the equivalence relation $\equiv_l$ $(mod\ H)$ ($\equiv_r$ $(mod\ H)$). Then $\hat{x} = xH = \{xh \mid h \in H\}$ ($\hat{x} = Hx = \{hx \mid h \in H\}$). We will call xH (Hx) the* left (right) coset *of x relative to H.*

Proof: We prove only one of them. We have that

$$\begin{aligned}
\hat{x} &= \{y \in G \mid x \equiv_l y \; (mod\, H)\} \\
&= \{y \in G \mid x^{-1}y \in H\} \\
&= \{y \in G \mid x^{-1}y = h,\ h \in H\} \\
&= \{y \in G \mid y = xh,\ h \in H\} \\
&= \{xh \in G \mid h \in H\} = xH.
\end{aligned}$$

▮

Proposition 2.5.3 *The map*

$$\varphi : G/\equiv_l (mod\ H) \longrightarrow G/\equiv_r (mod\ H),$$

defined by $\varphi(xH) = Hx^{-1}$, is a bijection.

Proof: We first need to show that φ is well defined. Indeed, if $xH = yH$, then $x^{-1}y \in H$, so $(x^{-1}y)^{-1} = y^{-1}(x^{-1})^{-1} \in H$, and hence $Hy^{-1} = Hx^{-1}$. Now define $\psi : G/\equiv_r (mod\ H) \longrightarrow G/\equiv_l (mod\ H)$ by $\psi(Hx) = x^{-1}H$. The fact that ψ is well defined is checked as above. It is clear that $\varphi(\psi(Hx)) = Hx$ and $\psi(\varphi(xH)) = xH$ for all $x \in G$, so φ and ψ are bijections inverse to each other. ▮

We will now see why the notion of normal subgroup is so important.

Theorem 2.5.4 *Let G be a group and $H \leq G$. The following assertions are equivalent:*
i) H is a normal subgroup.
ii) The two equivalence relations defined by H coincide: for $x, y \in G$ we have

$$x \equiv_l y \; (mod\, H) \Longleftrightarrow x \equiv_r y \; (mod\, H).$$

Proof: i) ⇒ ii). Assume that $H \trianglelefteq G$ and $x^{-1}y \in H$. Then $x(x^{-1}y)x^{-1} \in H$, so $yx^{-1} \in H$, and therefore $xy^{-1} \in H$. The fact that $xy^{-1} \in H \Rightarrow x^{-1}y \in H$ is proved similarly.
ii) ⇒ i). Let $x \in G$ and $h \in H$. We want to prove that $xhx^{-1} \in H$. We know that $xH = Hx$, so $xh = h_1x$ for some $h_1 \in H$. It follows that $xhx^{-1} = h_1xx^{-1} = h_1 \in H$, and the proof is complete. ∎

If $H \trianglelefteq G$ it follows from Proposition 2.5.4 that the factor sets with respect to the two identical equivalence relations defined by H coincide. Our notation for this factor set will be G/H.
Recall from Exercise 1.5.3 that a function f defined on a set M also defines an equivalence relation $\mathcal{R}_f$ on M. We now consider the analog situation for groups.

Proposition 2.5.5 *Let $f : G \longrightarrow G'$ be a morphism of groups. Then $\mathcal{R}_f$ coincides with the equivalence relation defined by the normal subgroup $Ker(f)$ on G.*

Proof: For $x, y \in G$, we have that $x\mathcal{R}_f y$ if and only if $f(x) = f(y)$ if and only if $f(x)f(y)^{-1} = 1_G$ if and only if $f(x)f(y^{-1}) = 1_G$ if and only if $f(xy^{-1}) = 1_G$ if and only if $xy^{-1} \in Ker(f)$. ∎

Proposition 2.5.6 *If $H \trianglelefteq G$, G/H is a group, and the canonical surjection from G to G/H is a group morphism.*

Proof: We have that $can : G \longrightarrow G/H$ sends $x \in G$ to $Hx = xH$. We define the operation on G/H by $(xH)(yH) = (xy)H$. We check that the operation is well defined. Let $x'H = xH$ and $y'H = yH$. Then $(xy)^{-1}(x'y') = y^{-1}x^{-1}x'y' = y^{-1}h_1y' = y^{-1}y'h_2$ for some $h_1, h_2 \in H$. Therefore $(xy)^{-1}(x'y') \in H$, and so $(xy)H = (x'y')H$.
It is easy to see that G/H is a group with this operation, and the definition ensures that *can* is a morphism of groups. Note that the inverse of xH in G/H is $x^{-1}H$, and $1_{G/H} = H$. ∎

Definition 2.5.7 *The group G/H defined in Proposition 2.5.6 is called the* factor group *of the group G relative to the normal subgroup H.*

As in the case of factor sets, we can define the factor group without any reference to elements: we will say that a factor group of the group G is a pair (N, p), where N is a group and $p : G \longrightarrow N$ is a surjective group morphism. Again as in the case of sets, it turns out that the two definitions are equivalent. One implication follows from Proposition 2.5.5. The other one follows from a result similar to Theorem 1.6.3:

Theorem 2.5.8 (The Universal Property of the Factor Group) *Let (N, p) be a factor group of the group G, let X be a group and $f : G \longrightarrow X$ a group morphism.*
i) There exists a group morphism $u : N \longrightarrow X$ such that $f = up$, which means that the diagram

$$\begin{tikzcd}
G \arrow[r, "p"] \arrow[dr, "f"'] & N \arrow[d, "u"] \\
& X
\end{tikzcd}$$

is commutative, if and only if $Ker(p) \subseteq Ker(f)$. If u exists, then it is unique.
If u as in i) exists, then:
ii) u is surjective if and only if f is surjective.
iii) u is injective if and only if $Ker(p) = Ker(f)$.

Proof: Using Theorem 1.6.3 and Proposition 2.5.5 we see that the only thing left to prove is that if a function u as in the statement exists, then it is a group morphism. Let $x', y' \in N$, and $x, y \in G$ such that $p(x) = x'$ and $p(y) = y'$. Then $u(x'y') = u(p(x)p(y)) = u(p(xy)) = f(xy) = f(x)f(y) = u(p(x))u(p(y)) = u(x')u(y')$. ∎

Corollary 2.5.9 *If (N_1, p_1) and (N_2, p_2) are two factor groups of G such that $Ker(p_1) = Ker(p_2)$, then there exists an isomorphism $u : N_1 \longrightarrow N_2$ such that $up_1 = p_2$.*

Proof: Take $(N, p) = (N_1, p_1)$, $X = N_2$ and $f = p_2$ in Theorem 2.5.8. ∎

Corollary 2.5.10 *If (N, p) is a factor group of G, then there exists an isomorphism $u : N \longrightarrow G/Ker(p)$ such that $u \circ p$ is the canonical surjection.*

Proof: Take $(N_1, p_1) = (N, p)$ and $(N_2, p_2) = (G/Ker(p), can)$, where $can : G \longrightarrow G/Ker(p)$, $can(x) = xKer(p)$. Then $Ker(can) = Ker(p)$ and we can apply Corollary 2.5.9. ∎

Corollary 2.5.11 (The First Isomorphism Theorem for Groups) *Let $f : G \longrightarrow G'$ be a group morphism. Then*

$$G/Ker(f) \simeq Im(f).$$

Proof: Use Corollary 2.5.10 for $(Im(f), f)$. ∎

Exercise 2.5.12 *Any cyclic group is isomorphic to a $\mathbb{Z}_n$.*

Solution: If G is cyclic, then

$$G =< a >= \{a^k \mid k \in \mathbb{Z}\},$$

and it is easy to check that the function

$$f : \mathbb{Z} \longrightarrow G, \;\; f(k) = a^k,$$

is a surjective group morphism. Consequently, $G \simeq \mathbb{Z}/Ker(f)$ by Corollary 2.5.11.

2.6 Lecture 2.6: Finite groups, 1

A finite group is a group G such that the set G is finite.

Definition 2.6.1 *Let G be a group. The* order *of the group G, if G is finite, is equal to the number of elements of G. If G has n elements, we will write $|G| = n$. If G is infinite we say that G has infinite order, and we write $|G| = \infty$.*

We saw in Proposition 2.5.3 that the set of left cosets of a group relative to a subgroup is in a bijection with the set of right cosets. This allows us to give the following:

Definition 2.6.2 *Let G be a group, and $H \leq G$. The* index *of H in G, is equal to the number of left (or right) cosets of G relative to H, if there are finitely many such cosets. If there are n cosets, we will write $|G : H| = n$. If there are infinitely many cosets we say that H has infinite index in G, and we write $|G : H| = \infty$. Note that if $H \trianglelefteq G$, then the order of the factor group G/H coincides with the index of H in G: $|G/H| = |G : H|$.*

It is clear that any subgroup of a finite group is finite and has finite index. An infinite group can have finite subgroups ($\{1, -1\} \leq (0, \infty)$), or subgroups of finite index ($|\mathbb{Z} : n\mathbb{Z}| = n$ if $n > 0$).

Exercise 2.6.3 *A subgroup of index two is normal.*

Theorem 2.6.4 *Let G be a finite group, and $H \leq G$. Then*

$$|G| = |H|\,|G : H|\,.$$

Proof: G is equal to the union of the left cosets relative to H, and the cosets are disjoint, so the order of G is equal to the sum of elements of the left cosets. In each left coset xH there are $|H|$ elements, because the function $\varphi : H \longrightarrow xH$, $\varphi(h) = hx$ is bijective (it is clearly surjective, and it is also injective by the cancelation law). On the other hand, there are exactly $|G : H|$ cosets, so the result follows. ∎

Corollary 2.6.5 *The order of a subgroup of a finite group divides the order of the group.*

We now give a second definition for the order of an element in a group. We will see soon that the two definitions

Definition 2.6.6 *Let G be a group and $a \in G$. The* order *of a is the order of $< a >$, the cyclic subgroup generated by a (recall that $< a >= \{a^k \mid k \in \mathbb{Z}\}$). We write $|a| = |< a >|$.*

Exercise 2.6.7 *Let G be a finite group and $a \in G$. Then:*
i) the order of a divides the order of G.
ii) $|a| = 1$ if and only if $a = 1_G$.
iii) $|a| = \left|a^{-1}\right|$.

Solution: i) The order of a is the order of the subgroup generated by a, so the assertion follows from the Lagrange theorem.
ii) The subgroup generated by a is equal to $\{1_G\}$ if and only if $a = 1_G$.
iii) $a^k = 1_G \Leftrightarrow (a^{-1})^k = 1_G$.

We now see that Definitions 2.6.6 and 2.2.8 define the same thing.

Proposition 2.6.8 *Let $a \in G$, $|a| = n$. Then n is the smallest element of the set $\{m \in \mathbb{N} \mid a^m = 1_G\}$.*

Proof: Since $|a| = n$, it follows that $< a >= \{1_G, a, a^2, \ldots, a^{n-1}\}$ has n elements, i.e. the elements $1_G, a, a^2, \ldots, a^{n-1}$ are distinct, so in particular $a^k \neq 1_G$ if $0 < k < n$. Since we know that $a^n \in < a >$, it follows that $a^n = 1_G$, and the assertion is proved. ∎

Proposition 2.6.9 *A group of order 6 is isomorphic to $\mathbb{Z}_6$ or S_3.*

Proof: If G is cyclic, then G is isomorphic to $\mathbb{Z}_6$. If G is not cyclic, there are no elements of order 6, so all elements different from 1_G have order 2 or 3. If all elements have order 2, and we pick two such elements, x and y, then xy also has order 2, so $xyxy = 1_G$, and multiplying this equality by x on the left and y on the right we get $yx = xy$. It follows that $\{1_G, x, y, xy\} \leq G$, so by the Lagrange theorem $4 \mid 6$, a contradiction. It follows that there exists an element $\theta \in G$ of order 3. Then $H = \{1_G, \theta, \theta^2\}$ has index 2, so it is normal. We prove that any element z in the complement of H has order 2. Indeed, $z^2 \in H$ (G/H has order 2), and if $z^2 = \theta$ or $z^2 = \theta^2$ we get that the order of z is 3 or 6. Since G is not cyclic, the order cannot be 6. If the order is 3 and $z^2 = \theta^2$, then $\theta^2 z = 1_G$, so $z = \theta$, a contradiction. Similarly, if $z^2 = \theta$ we get $z = \theta^2$, a contradiction. In conclusion, the order of z is 2. Let now $\tau \in G$, $\tau \notin H$. Then we know that the elements $\tau, \tau\theta, \tau\theta^2$ are distinct and not in H, so they all have order 2 and $G = \{1_G, \theta, \theta^2, \tau, \tau\theta, \tau\theta^2\}$. We have $\theta\tau = (\theta^2)^{-1}\tau^{-1} = (\tau\theta^2)^{-1} = \tau\theta^2$, and $\theta^2\tau = \theta^{-1}\tau^{-1} = (\tau\theta)^{-1} = \tau\theta$, and we can check that the group morphism $\varphi : S_3 \longrightarrow G$, $\varphi((12)) = \tau$ and $\varphi((123)) = \theta$ is an isomorphism. ∎

Exercise 2.6.10 *Prove that a group of order 4 is isomorphic to $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$.*

Solution: Let G be a group of order 4. If there exists an element of order 4, then the group is cyclic, hence isomorphic to $\mathbb{Z}_4$. If there are no elements of order 4, then all elements different from 1_G have order 2. Let x, y be two distinct such elements. Then the elements $1_G, x, y, xy$ are distinct, and hence $G = \{1_G, x, y, xy\}$. Then the map $f : G \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$, defined by $f(1_G) = (0, 0)$, $f(x) = (1, 0)$, $f(y) = (0, 1)$, and $f(xy) = (1, 1)$ is an isomorphism.

2.7 Lecture 2.7: Finite groups, 2

Proposition 2.7.1 *Let $a, b \in G$, $|a| = m$, $|b| = n$, and $ab = ba$. Then*
i) if $1 = (m, n)$, then $|ab| = mn$.
ii) It is not true in general that $|ab| = [m, n]$.

Proof: i) Let $k = |ab|$. It is clear that $(ab)^{mn} = a^{mn}b^{mn} = 1_G$, so $k \mid mn$. Now since $(ab)^k = a^k b^k = 1_G$, then $(ab)^{nk} = a^{nk}b^{nk} = a^{nk} = 1_G$. Then $m \mid nk$, and since $1 = (m, n)$ we have $m \mid k$ by Euclid's lemma. Similarly, $n \mid k$, and hence $mn = [m, n] \mid k$, so $mn = k$.
ii) Take $|a| = m > 1$, and $b = a^{-1}$. We clearly have $|b| = m$. Then $ab = ba = 1_G$ has order $1 \neq [m, m] = m$. ∎

Exercise 2.7.2 *Give an example to show that the conclusion of Proposition 2.7.1 i) is not true if $ab \neq ba$.*

Solution: The order of (12) in S_3 is 2, and the order of (123) is 3, but the order of $(12)(123) = (23)$ is 2.

Exercise 2.7.3 *Show that:*
i) $\mathbb{Z}_n \times \mathbb{Z}_m \simeq \mathbb{Z}_{nm} \Leftrightarrow 1 = (m, n)$.
ii) $n\mathbb{Z} \cap m\mathbb{Z} = [m, n]\mathbb{Z}$.
iii) $n\mathbb{Z} + m\mathbb{Z} = (m, n)\mathbb{Z}$.

Solution: i) If $1 = (m, n)$, the order of $(1, 0)$ is n, the order of $(0, 1)$ is m, and $(1, 0)$ and $(0, 1)$ commute, so the order of $(1, 1)$ is $[n, m] = nm$, i.e. $\mathbb{Z}_n \times \mathbb{Z}_m$ is cyclic of order nm, hence isomorphic to $\mathbb{Z}_{nm}$. Conversely, if $1 \neq (m, n)$, then there is a least common multiple $k = [m, n]$ such that $0 < k < nm$. For any $(a, b) \in \mathbb{Z}_n \times \mathbb{Z}_m$, we have $k(a, b) = (0, 0)$, so there are no elements of order nm in $\mathbb{Z}_n \times \mathbb{Z}_m$.
The right to left implication is known as the **Chinese Remainder Theorem**, and is usually given in this form: if $1 = (m, n)$, then the system of two congruences $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$ has a solution. A constructive proof of this statement goes like this: since $1 = (m, n)$ we have $1 = m(m^{-1})_{(mod\ n)} + n(n^{-1})_{(mod\ m)}$. A solution to the first congruence is of the form $mt + a$, and we find t by asking it to also be a solution to the second congruence: $mt + a \equiv b \pmod{n}$, so $t = (m^{-1})_{(mod\ n)}(b - a)$, and a solution to the system will be congruent to $m(m^{-1})_{(mod\ n)}(b - a) + a \pmod{mn}$. Collecting terms in a and b and replacing $1 - m(m^{-1})_{(mod\ n)} = n(n^{-1})_{(mod\ m)}$ produces the more symmetric system solution $n(n^{-1})_{(mod\ m)}a + m(m^{-1})_{(mod\ n)}b \pmod{mn}$.
ii) Let $n\mathbb{Z} \cap m\mathbb{Z} = k\mathbb{Z}$. We will show that $k = [m, n]$. Obviously $k\mathbb{Z} \subseteq n\mathbb{Z}$ and $k\mathbb{Z} \subseteq m\mathbb{Z}$, so $n \mid k$ and $m \mid k$. Now if $n \mid l$ and $m \mid l$, then $l\mathbb{Z} \subseteq n\mathbb{Z}$ and $l\mathbb{Z} \subseteq m\mathbb{Z}$, so $l\mathbb{Z} \subseteq n\mathbb{Z} \cap m\mathbb{Z} = k\mathbb{Z}$, so $k \mid l$.

iii) Let $n\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z}$. We show that $d = (a, b)$. Since $n\mathbb{Z} \subseteq d\mathbb{Z}$ and $m\mathbb{Z} \subseteq d\mathbb{Z}$, it follows that $d \mid n$ and $d \mid m$. Now if $s \mid n$ and $s \mid m$, it follows that s divides any linear combination of n and m, in particular $s \mid d$.

Exercise 2.7.4 *Let $(a_1 a_2 \dots a_k) \in S_n$ be a cycle of length k. Show that $|(a_1 a_2 \dots a_k)| = k$.*

Solution: Let $\sigma = (a_1 a_2 \dots a_k)$. Then $\sigma^2(a_1) = a_3$, $\sigma^3(a_1) = a_4$, $\dots$ $\sigma^{k-1}(a_1) = a_k$, and $\sigma^k = Id$.

Exercise 2.7.4 provides a quick way to find the order of a permutation in S_n. We first write the permutation as a product of disjoint cycles, then, since disjoint cycles commute, we find the order of the permutation as the least common multiple of the lengths of those cycles.

Exercise 2.7.5 *Find the order of*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 6 & 5 & 8 & 1 & 2 & 10 & 7 & 9 & 4 \end{pmatrix} \in S_{10}.$$

Solution: We have that $\sigma = (135)(26)(487\,10)$, so $|\sigma| = [3, 2, 4] = 12$.

We now define the signature of a permutation. For any $\sigma \in S_n$, define

$$\varepsilon(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(i) - \sigma(j)}{i - j}.$$

If $\sigma, \tau \in S_n$ we have

$$\varepsilon(\sigma\tau) = \prod_{1 \le i < j \le n} \frac{\sigma\tau(i) - \sigma\tau(j)}{i - j} =$$

$$= \prod_{1 \le i < j \le n} \frac{\tau(i) - \tau(j)}{i - j} \cdot \frac{\sigma\tau(i) - \sigma\tau(j)}{\tau(i) - \tau(j)} = \varepsilon(\sigma)\varepsilon(\tau).$$

Therefore

$$\varepsilon : S_n \longrightarrow \{1, -1\}$$

is a group morphism. This morphism is surjective, the identity is sent to one, and any transposition is sent to -1. The permutations in the kernel of this morphism (denoted by A_n and called the *alternating group*) are called *even*, and the other ones are called *odd*. To see why they are called even and odd, consider a cycle in S_n of length k, and write it as a product of transpositions like this:

$$(i_1 i_2 \dots i_k) = (i_1 i_k)(i_1 i_{k-1}) \dots (i_1 i_3)(i_1 i_2).$$

Therefore any even (odd) permutation can be written as a product of an even (odd) number of transpositions. In particular, a cycle is even if and only if it has odd length.

The next important result is Cayley's theorem.

Exercise 2.7.6 *Let G be a group. Prove that the map $\varphi : G \longrightarrow S(G)$ sending $x \in G$ to $\varphi(x) : G \longrightarrow G$, $\varphi(x)(g) = xg$ is an injective morphism of groups.*

Solution: First we have that $\varphi(xy)(g) = (xy)g = x(yg) = \varphi(x)(yg) = \varphi(x)(\varphi(y)(g)) = \varphi(x)\varphi(y)(g)$ for all $g \in G$, so $\varphi(xy) = \varphi(x)\varphi(y)$, i.e. φ is a group morphism. Now if $x \in Ker(\varphi)$, it follows that $\varphi(x) = Id_G$, in particular $\varphi(x)(1_G) = x1_G = 1_G$. Therefore $x = 1_G$, i.e. $Ker(\varphi) = \{1_G\}$, so φ is injective.

Historically, the first studied groups were groups of permutations (of solutions of polynomial equations). Groups also arise naturally as symmetries of various geometric objects. The group of symmetries of a plane figure consist of all the transformations applied to a cutout of that figure after we take it out of a board before putting it back in the hole. It is clear that the options that we have before putting the cutout back are rotations, or flips, or combinations of these. We call these transformations symmetries, and the operation is composition. Let us look at a few examples.

We start with the symmetries of a rectangle. Once we cut the rectangle from a board and we take it out, we have the following options before we put it back in: do nothing, just put it back, we denote this by I. Rotate the rectangle by π (left or right, it's the same transformation), we denote this by R. Flip it upside down, we denote this by F. Twist it left to right or right to left, we call this T. Combining all these gives the following table for this group

$\circ$	I	R	F	T
I	I	R	F	T
R	R	I	T	F
F	F	T	I	R
T	T	F	R	I

This group is called the Klein Four Group, is usually denoted by V_4 and is easily seen to be isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

The final two examples are particular cases of dihedral groups, which were defined at the end of Section 2.2. First we find the group of symmetries of an equilateral triangle, which is called the dihedral group D_3. If we denote by 1 the identity transformation (does nothing), by θ the counterclockwise rotation of $\frac{2\pi}{3}$ about the center of the triangle, and by τ the flip along one of the heights of the triangle, then we can check that

$$D_3 = \{1, \theta, \theta^2, \tau, \theta\tau, \theta^2\tau\},$$

$\theta^3 = \tau^2 = 1$, $\tau\theta = \theta^2\tau$, so $D_3 \simeq S_3$ as in the proof of Proposition 2.6.9. Another way to see this is to mark the vertices of the cutout and the vertices of the hole by $\cdot$, $\cdot\cdot$, and $\cdots$ (we use these rather than 1, 2, and 3 so that they can be read from the other side as well), and note that the transformations of the triangle correspond in fact to the permutations of the vertices.

The group of transformations of a square, which is called the dihedral group D_4, is obtained as follows: we denote by θ the counterclockwise rotation of $\frac{\pi}{2}$ about the center of the square, and by τ the flip along one of the perpendiculars from the center to one of the sides, then we can check that

$$D_4 = \{1, \theta, \theta^2, \theta^3, \tau, \theta\tau, \theta^2\tau, \theta^3\tau\},$$

$\theta^4 = \tau^2 = 1$, $\tau\theta = \theta^3\tau$.

Chapter 3

Part III

3.1 Lecture 3.1: Rings

We continue the process started in Part II: there we started with a set and considered an operation on that set. Now we are starting with a group and consider a second operation on it.

Definition 3.1.1 *A* ring *is a set R with at least two elements, 0_R and 1_R, and two operations, $+$ and $\cdot$, called* addition *and* multiplication*, such that the following conditions hold:*
i) $(R, +)$ is an abelian group with identity element 0_R.
ii) Multiplication is associative and has identity element 1_R. This means that for all $a, b, c \in R$ we have:

$$a(bc) = (ab)c \text{ and } a1_R = 1_Ra = a.$$

iii) Multiplication is distributive with respect to addition, i.e. for all $a, b, c \in R$ we have:

$$a(b + c) = ab + ac \text{ and } (a + b)c = ac + bc.$$

If multiplication is commutative, we say that the ring is commutative.

Exercise 3.1.2 *Let $(R, +, \cdot)$ be a ring. Then the following hold:*
i) $a0_R = 0_Ra = 0_R$ for all $a \in R$.
ii) Rule of signs: $a(-b) = (-a)b = -ab$, and $(-a)(-b) = ab$.
iii) $a(b_1 + b_2 + \ldots + b_n) = ab_1 + ab_2 + \ldots + ab_n$ and $(b_1 + b_2 + \ldots + b_n)a = b_1a + b_2a + \ldots + b_na$ for all $n \geq 2$ and $a, b_1, b_2, \ldots, b_n \in R$.

Solution: i) $a0_R = a(0_R + 0_R) = a0_R + a0_R$, and after adding $-a0_R$ to both sides we get $a0_R = 0_R$. The equality $0_Ra = 0_R$ is proved similarly.
ii) $0_R = a0_R = a(b - b) = ab + a(-b)$, so $a(-b) = -ab$. The proof of $(-a)b = -ab$ is similar. Now $(-a)(-b) = (-(-a))b = ab$.
iii) Use induction on n. For $n = 2$ we have $a(b_1 + b_2) = ab_1 + ab_2$ which is the distributivity law. If the assertion is true for n, then $a(b_1 + \ldots + b_n + b_{n+1}) = a(b_1 + \ldots + b_n) + ab_{n+1} = ab_1 + \ldots + ab_n + ab_{n+1}$.

Definition 3.1.3 *An element a in a ring R is called* invertible *(or a* unit*), if it has an inverse with respect to multiplication, i.e. there exists $a' \in R$ such that $aa' = a'a = 1_R$. The inverse of a unit $a \in R$ is unique (see Exercise 2.1.4 ii)) and will be denoted by a^{-1}. The set of units of the ring R will be denoted by $U(R)$.*
An element a in a ring R is called a left zero divisor *if there exists $b \in R$, $b \neq 0_R$, such that $ab = 0_R$. Similarly, a will be a* right zero divisor *if there exists $b \in R$, $b \neq 0_R$, such that $ba = 0_R$.*

Exercise 3.1.4 *Let $(R, +, \cdot)$ be a ring. Then:*
i) 0_R is a zero divisor (left and right).
ii) if $a \in R$ is a unit, a is not a zero divisor (left or right).
iii) if $a \in R$ is a zero divisor, a is not a unit.
iv) $(U(R), \cdot)$ is a group.

Solution: i) $0_R1_R = 1_R0_R = 0_R$.
ii) Assume that a is a unit, and let $ab = 0_R$. After multiplying by a^{-1} on the left, we get $b = 0_R$. Similarly, if $ba = 0_R$, then $b = 0_R$.
iii) is logically equivalent to ii).
iv) Multiplication is associative, $1_R \in U(R)$, and all elements in U have inverses.

Definition 3.1.5 *A commutative ring F is called a* field *if any non-zero element of R is a unit (i.e. $U(F) = F^* = F \setminus \{0_F\}$). A commutative ring D is called a* domain *if D has no zero divisors other than 0_D.*

We give now some examples of rings, but leave the verification as an exercise.

Example 3.1.6 *The following are examples of rings. Which ones are commutative? Which ones are domains? Which ones are fields?*
$(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, the set of 2×2 matrices with complex entries, with the addition and multiplication of matrices: $(M_2(\mathbb{C}), +, \cdot)$, $(\mathbb{Z}_n, +, \cdot)$.

Definition 3.1.7 *Let R and R' be rings, and $f : R \longrightarrow R'$. We say that f is a* ring morphism *if the following hold:*
i) f is a group morphism, i.e. $f(x + y) = f(x) + f(y)$ for all $x, y \in R$.
ii) $f(xy) = f(x)f(y)$ for all $x, y \in R$.
iii) $f(1_R) = 1_{R'}$.
The morphism f is said to be an injective morphism if the function f is injective. Similarly, if the function f is surjective, we say that f is a surjective morphism. A ring morphism $f : R \longrightarrow R'$ is called an isomorphism *if there exists a ring morphism $f' : R' \longrightarrow R$ such that $f \circ f' = Id_{R'}$ and $f' \circ f = Id_R$; we then say that the rings R and R' are* isomorphic, *and we write $R \simeq R'$. A morphism from R to R is called an* endomorphism *of R, and an isomorphism from R to R is called an* automorphism *of R.*

We remark that since f is a group morphism, it is automatic that $f(0_R) = 0_{R'}$. For ring morphisms we have to ask that $f(1_R) = 1_{R'}$, because it does not follow from the other two conditions. Indeed, the constant map 0_R from R to R satisfies i) and ii) from Definition 3.1.7, but not iii).

Definition 3.1.8 *Let R_1 and R_2 be rings, and define the following operations on the cartesian product $R_1 \times R_2$: $(x, y)+(x', y') = (x+x', y+y')$ and $(x, y) \cdot (x', y') = (xx', yy')$, where $x, x' \in R_1$ and $y, y' \in R_2$. Then $R_1 \times R_2$ is a ring with these operations (it is called the* direct product *of the rings R_1 and R_2).*

The following properties of ring morphisms are left as exercises:

Exercise 3.1.9 *Let $f : R \longrightarrow R'$ and $g : R' \longrightarrow R''$ be ring morphisms. Then:*
i) if $x \in U(R)$, then $f(x) \in U(R')$, and we have $f(x^{-1}) = f(x)^{-1}$.
ii) gf is a ring morphism.
iii) f is an isomorphism if and only if f is bijective.

Solution: i) We have that $1_{R'} = f(1_R) = f(xx^{-1}) = f(x)f(x^{-1})$.
ii) and iii). We already know from groups that addition is preserved. The proof for multiplication is identical.

Definition 3.1.10 *The characteristic of a ring R is the order of 1_R in the group $(R, +)$.*

3.2 Lecture 3.2: Subrings and ideals

In this lecture we introduce two notions that are the analogs for rings of the notions of subgroup and normal subgroup. We begin by the following:

Definition 3.2.1 *Let R be a ring, and S a nonempty subset of R. Then S is called a* subring *of R if the operations on R induce on S a ring structure.*

A trivial example of a subring in any ring R is R itself. When checking that a certain subset S of a ring R is a subring we need to check three conditions:
SR1) If $x, y \in S$, then $x - y \in S$.
SR2) $1_R \in S$.
SR3) If $x, y \in S$, then $xy \in S$.
Note that SR2) ensures that S is not empty, and SR1) says that S is a subgroup of R. In conclusion, a subring of a ring is a subgroup that contains the identity and is closed under multiplication.

Example 3.2.2 *The following subsets are subrings: $\mathbb{Z} \subseteq \mathbb{Q}$, $\mathbb{Q} \subseteq \mathbb{R}$, $\mathbb{R} \subseteq \mathbb{C}$.*

Exercise 3.2.3 *Let $f : R \longrightarrow R'$ be a morphism of rings. Then:*
i) $f(R)$ is a subring of R' (as in the case of groups, we denote $f(R)$ by $Im(f)$ and call it the image of f).
ii) is $f^{-1}(0_{R'})$ a subring of R? (as in the case of groups, we denote $f^{-1}(0_{R'})$ by $Ker(f)$ and call it the kernel of f).
iii) If S is a subring of R, then $f(S)$ is a subring of R'.
iv) If S' is a subring of R', then $f^{-1}(S')$ is a subring of R.
v) f is surjective $\Leftrightarrow Im(f) = R'$.
vi) f is injective $\Leftrightarrow Ker(f) = \{0_R\}$.

Solution: i) is a subring. We know that $Im(f)$ is a subgroup of R'. We have that $1_{R'} = f(1_R) \in Im(f)$, and if $x', y' \in Im(f)$, then $x' = f(x)$ and $y' = f(y)$, and so $x'y' = f(x)f(y) = f(xy) \in Im(f)$.
ii) not a subring, $1_R \notin Ker(f)$.
iii) is a subring, the proof is similar to i).
iv) is a subring, we have $1_R \in f^{-1}(S')$. Then if $x, y \in f^{-1}(S')$, so $f(x+y) = f(x) + f(y) \in S'$, and $f(xy) = f(x)f(y) \in S'$, thus $x + y, xy \in f^{-1}(S')$.
v) is just the definition of surjectivity.
vi) follows from Exercise 2.3.8 vi), because f is in particular a morphism of groups.

We now introduce an important notion that plays the same role for rings that normal subgroups play for groups.

Definition 3.2.4 *Let R be a ring and I a nonempty subset of R. We will say that I is a* left ideal *of R if I is a subgroup of R and it is closed under left multiples. This means that the following conditions are satisfied:*
LI1) for any $x, y \in I$ we have $x - y \in I$.
LI2) for any $x \in I$ and $r \in R$ we have $rx \in I$.
We will say that I is a right ideal *of R if I is a subgroup of R and it is closed under right multiples. This means that the following conditions are satisfied:*
RI1) for any $x, y \in I$ we have $x - y \in I$.
RI2) for any $x \in I$ and $r \in R$ we have $xr \in I$.
An ideal that is both a left and a right ideal is called two-sided*. Properties LI2) and RI2) are called absorption properties.*

Trivial examples of two-sided ideals in any ring R are $\{0_R\}$ and R itself. An ideal different from R is called *proper*.

Exercise 3.2.5 *i) A subring of R that is also an ideal (left or right) has to be equal to R.*
ii) In general, the ideal I of R is equal to $R \Leftrightarrow I$ contains a unit.

Solution: i) If $1_R \in I$, then any $r \in R$ will be in I, since it can be written as $r = r1_R$ or $r = 1_R r$, so $I = R$.
ii) If $I = R$, then $1_R \in I$ is a unit. Conversely, if $x \in I$ is a unit, then $1_R = xx^{-1} = x^{-1}x$, so $1_R \in I$, thus $I = R$ by i).

Corollary 3.2.6 *Let F be a commutative ring. The following assertions are equivalent:*
i) F is a field.
ii) The only ideals of F are $\{0_F\}$ and F.

Example 3.2.7 *The following subsets are ideals:*
i) If $n \in \mathbb{Z}$, $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\} \subseteq \mathbb{Z}$ is an ideal, so all subgroups of $\mathbb{Z}$ are ideals.
ii) If R is a commutative ring, and $x_1, x_2, \ldots, x_n \in R$, then

$$I = Rx_1 + Rx_2 + \ldots + Rx_n = \{a_1x_1 + a_2x_2 + \ldots + a_nx_n \mid a_i \in R, 1 \leq i \leq n\}$$

is an ideal of R, called the ideal generated *by $x_1, x_2, \ldots, x_n$. If $n = 1$, Rx_1 is called the* principal ideal *generated by x_1.*

Definition 3.2.8 *A domain in which all ideals are principal is called a* Principal Ideal Domain *(or PID).*

Remark 3.2.9 *In $\mathbb{Z}$ and $\mathbb{Z}_n$ all ideals are principal.*

We end this section with the study of the behavior of ideals through ring morphisms.

Proposition 3.2.10 *Let $f : R \longrightarrow R'$ be a ring morphism. Then the following assertions hold:*
i) If I' is a left ideal of R', then $f^{-1}(I')$ is a left ideal of R, and the same is true if we replace "left" by "right" or "two-sided".
ii) If f is surjective and I is a left ideal of R, then $f(I)$ is a left ideal of R', and the same is true if we replace "left" by "right" or "two-sided".
iii) $Ker(f)$ is a two-sided ideal of R.

Proof: i) We know from Exercise 2.3.8 iv) that $f^{-1}(I') \leq R$. Let $r \in R$ and $x \in f^{-1}(I')$. We know that $f(x) \in I'$ and we want to prove that $f(rx) \in I'$. We have $f(rx) = f(r)f(x) \in I'$, because I' is a left ideal of R'. The proof of the other two assertions is similar.
ii) We know from Exercise 2.3.8 iii) that $f(I) \leq R'$. Let $r' \in R'$ and $x' \in f(I)$. Then $x' = f(x)$ for some $x \in I$, and since f is surjective, $r' = f(r)$ for some $r \in R$. We then have $r'x' = f(r)f(x) = f(rx) \in f(I)$, since I is a left ideal of R. The proof of the other two assertions is similar.
iii) follows from i), because $\{0_{R'}\}$ is a two-sided ideal of R'. ∎

3.3 Lecture 3.3: Factor rings

Let G be a group and $H \trianglelefteq G$. Recall that this means that $xH = Hx$ for all $x \in G$, or, equivalently, that the two congruences modulo H, left and right, coincide:

$$x \equiv y(mod\ H) \Leftrightarrow xy^{-1} \in H \Leftrightarrow x^{-1}y \in H.$$

This also meant that congruence modulo H is compatible with the group operation, i.e. we can multiply congruences: if $x \equiv y(mod\ H)$ and $z \equiv w(mod\ H)$, then $xz \equiv yw(mod\ H)$, because $zw^{-1} = h \in H$, $xh = h_1x$ for some $h_1 \in H$, and $xy^{-1} = h_2 \in H$, so $xz(yw)^{-1} = xzw^{-1}y^{-1} = xhy^{-1} = h_1xy^{-1} = h_1h_2 \in H$. This is equivalent to the fact that multiplication of congruence classes (or cosets) relative to H is well defined, or the canonical surjection from G to G/H is a group morphism.
Let now R be a ring and I a two-sided ideal of R. In particular, I is a subgroup of the abelian group R (under addition), so I is a normal subgroup of R. In conclusion, we can introduce a group structure on the factor group R/I like this:

$$(x + I) + (y + I) = (x + y) + I,\ \ x, y \in R,$$

so R/I is a group under the addition defined above, and the canonical surjection $can : R \longrightarrow R/I$ is a surjective group morphism. The zero element of this group is $0_{R/I} = 0 + I = I$. The fact that I is a two-sided ideal allows us to define multiplication on R/I like this:

$$(x + I)(y + I) = xy + I,\ \ x, y \in R.$$

In order to show that this multiplication is well defined, we need to show that if $x - x' \in I$ and $y - y' \in I$, then $xy - x'y' \in I$. Now $xy - x'y' = xy - xy' + xy' - x'y' = x(y - y') + (x - x')y' \in I$, because both $x(y - y')$ and $(x - x')y'$ belong to I (note that both left and right absorption properties were used). In this way R/I becomes a ring with identity $1_{R/I} = 1 + I$. The fact that the ring axioms are verified follows from the definition of the operations and the fact that R is a ring. For example left distributivity is checked as follows:

$$\begin{aligned}(x + I)((y + I) + (z + I)) &= (x + I)(y + z + I)\\ &= x(y + z) + I\\ &= xy + xz + I\\ &= (xy + I) + (xz + I)\\ &= (x + I)(y + I) + (x + I)(z + I).\end{aligned}$$

Definition 3.3.1 *If R is a ring, and I is a two-sided ideal of R, the ring R/I constructed above is called the* factor ring *of R relative to I.*

As in the case of sets or groups, we can define factor rings without any reference to elements:

Definition 3.3.2 *A factor ring of the ring R is a pair (N, p), where N is a ring, and $p : R \longrightarrow N$ is a surjective ring morphism.*

Since $can : R \longrightarrow R/I$ is a surjective ring morphism, a factor ring in the sense of Definition 3.3.1 is also a factor ring in the sense of Definition 3.3.2. The fact that the two definitions are equivalent will follow, as in the case of sets or groups, from a universal property.

Theorem 3.3.3 (The Universal Property of the Factor Ring) *Let (N, p) be a factor ring of the ring R, let X be a ring and $f : R \longrightarrow X$ a ring morphism.*
i) There exists a ring morphism $u : N \longrightarrow X$ such that $f = up$, which means that the diagram

$$\begin{tikzcd}
R \arrow[r, "p"] \arrow[dr, "f"'] & N \arrow[d, "u"] \\
 & X
\end{tikzcd}$$

is commutative, if and only if $Ker(p) \subseteq Ker(f)$. If u exists, then it is unique.
If u as in i) exists, then:
ii) u is surjective if and only if f is surjective.
iii) u is injective if and only if $Ker(p) = Ker(f)$.

Using Theorem 2.5.8 we see that the only thing left to prove is that if a group morphism u as in the statement exists, then it is a ring morphism. Since f is a ring morphism, the proof is identical to the one of Theorem 2.5.8.

Corollary 3.3.4 *If (N_1, p_1) and (N_2, p_2) are two factor rings of R such that $Ker(p_1) = Ker(p_2)$, then there exists an isomorphism $u : N_1 \longrightarrow N_2$ such that $up_1 = p_2$.*

Corollary 3.3.5 *If (N, p) is a factor ring of R, then there exists an isomorphism $u : N \longrightarrow R/Ker(p)$ such that $u \circ p$ is the canonical surjection.*

Corollary 3.3.6 (The First Isomorphism Theorem for Rings) *Let $f : R \longrightarrow R'$ be a ring morphism. Then*

$$R/Ker(f) \simeq Im(f).$$

Exercise 3.3.7 *Let $n > 0$ be an integer.*
i) Describe the units of the ring $\mathbb{Z}_n$.
ii) Describe the zero divisors of the ring $\mathbb{Z}_n$.
iii) (Euler's Theorem) If a is an integer and $1 = (a, n)$, then $a^{\varphi(n)} \equiv 1(mod\ n)$, where $\varphi(n)$ is the Euler function, $\varphi(0) = 0$, $\varphi(1) = 1$, and if $m > 1$, $\varphi(m) =$ number of natural numbers relatively prime to m and less than m.
iv) Show that $\mathbb{Z}_n \times \mathbb{Z}_m \simeq \mathbb{Z}_{nm}$ as rings $\Leftrightarrow 1 = (n, m)$.
v) φ is multiplicative, i.e. $\varphi(nm) = \varphi(n)\varphi(m)$ if $1 = (n, m)$.
vi) $\varphi(p^k) = p^k - p^{k-1}$.
vii) If $n = p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}$ and p_i are distinct primes, $1 \leq i \leq s$, then

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_s}\right).$$

viii) (Fermat's Little Theorem) If p is a positive prime and a is an integer, then $a^p \equiv a(mod\ p)$.

Solution: i) (See Exercise 2.2.2 iii)). The units of $\mathbb{Z}_n$ are denoted by $\mathbf{U}_n$, they consist of those $a \in \mathbb{Z}_n$ with the property that $1 = (a, n)$, and they form an abelian group under multiplication. We have that $a \in \mathbb{Z}_n$ is a unit if and only if $au = 1$ for some u, if and only if $n \mid 1 - au$ if and only if $1 - au = nv$ for some v, if and only if $1 = au + nv$ if and only if $1 = (a, n)$.
ii) If $a \in \mathbb{Z}_n$ is not a unit, then it is a zero divisor. Indeed, if $a \in \mathbb{Z}_n$ is not a zero divisor, then the map $f : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$, $f(b) = ab$ is injective, because if $ab_1 = ab_2$, then $a(b_1 - b_2) = 0$, so $b_1 - b_2 = 0$, or $b_1 = b_2$. Since $\mathbb{Z}_n$ is finite, f is also surjective, so there exists a b such that $ab = 1$, i.e. a is a unit. Consequently, by Exercise 3.1.4 iii), the zero divisors in $\mathbb{Z}_n$ are precisely the non-units: $\{a \in \mathbb{Z}_n \mid 1 \neq (a, n)\}$.
iii) By i), the order of the group $\mathbf{U}_n$ is $\varphi(n) = |\mathbf{U}_n|$. If $1 = (a, n)$, then $\hat{a}$ is an element of the group, hence its order divides the order of the group, i.e. $\varphi(n)$, by Exercise 2.6.7 i), and the result follows.
iv) If $\mathbb{Z}_n \times \mathbb{Z}_m \simeq \mathbb{Z}_{nm}$ as rings, they are also isomorphic as groups, so $1 = (n, m)$ by Exercise 2.7.3 i). Conversely, if $1 = (n, m)$, then the map $f : \mathbb{Z}_{nm} \longrightarrow \mathbb{Z}_n \times \mathbb{Z}_m$, $f(\hat{a}(mod\, nm)) = (\hat{a}(mod\, n), \hat{a}(mod\, m))$ is an injective ring morphism, hence an isomorphism (both sets have the same number

of elements).
v) Let $1 = (n, m)$. By iv) and the definition of multiplication in the direct product, we have that $\mathbf{U}_n \times \mathbf{U}_m \simeq \mathbf{U}_{nm}$. The left hand side has $\varphi(n)\varphi(m)$, and the right hand side has $\varphi(nm)$ elements, so the result follows.
vi) We count how many numbers between 1 and p^k are not relativley prime to p^k. These numbers are $p, 2p, 3p, p^{k-1}p = p^k$, so there are p^{k-1} of them. The rest, i.e. $p^k - p^{k-1}$, are relatively prime to p^k.
vii) Since the p_i are distinct primes, we apply v) $k-1$ times and we get $\varphi(p_1^{k_1}p_2^{k_2}\ldots p_s^{k_s}) = \varphi(p_1^{k_1})\varphi(p_2^{k_2}\ldots p_s^{k_s}) = \ldots = \varphi(p_1^{k_1})\varphi(p_2^{k_2})\ldots\varphi(p_s^{k_s})$. Then by vi) we get $\varphi(n) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1})\ldots(p_s^{k_s} - p_s^{k_s-1}) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_s}\right)$.
viii) We need to show that $p \mid a^p - a = a(a^{p-1} - 1)$. This is obviously true if p divides a. If p does not divide a, use iii) for $n = p$ to obtain that p divides $a^{p-1} - 1$. The result in the following exercise is known as Wilson's Theorem.

Exercise 3.3.8 *An integer $p > 1$ is prime if and only if $(p-1)! \equiv -1(mod\ p)$.*

Solution: If $p = 2$ the assertion is clear. If p is an odd prime, $\mathbf{U}_p = \{1, 2, \ldots, p-1\}$. If $a \in \mathbf{U}_p$ is equal to its own inverse, then $p \mid a^2 - 1 = (a+1)(a-1)$, so $a = p-1$, or $a = 1$. Therefore, in the product $(p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-1)$, each element appears with its inverse (with the exception of 1 and $p-1$, which are their own inverses. Therefore, $(p-1)! = 1 \cdot 1 \cdot 1 \cdots 1 \cdot (p-1)$ in $\mathbb{Z}_p$, or $(p-1)! \equiv -1(\text{mod } p)$.
Conversely, if $(p-1)! \equiv -1(\text{mod } p)$, it follows that p is not divisible by any prime less than $p-1$, so p is prime.

3.4 Lecture 3.4: Prime and maximal ideals

From now on, all rings will be commutative.

Definition 3.4.1 *An ideal P of the commutative ring R is said to be* prime *if $P \neq R$ and $ab \in P$ implies that $a \in P$ or $b \in P$.*

Remark 3.4.2 *i) We have that $\{0_R\}$ is a prime ideal if and only if R is a domain.*
ii) $\{0\}$ is a prime ideal of $\mathbb{Z}$.
iii) If $P \neq \{0\}$ is a prime ideal of $\mathbb{Z}$, then $P = p\mathbb{Z}$, where p is prime.

We now investigate how prime ideals behave relative to ring morphisms.

Proposition 3.4.3 *Let $f : R \longrightarrow R'$ be a ring morphism (recall that all rings are commutative).*
i) If P' is a prime ideal of R', then $P = f^{-1}(P')$ is a prime ideal of R.
ii) If f is surjective, and P is a prime ideal of R such that $Ker(f) \subseteq P$, then $P' = f(P)$ is a prime ideal of R'.

Proof: i) We first remark that $P \neq R$, because $1_R \notin P = f^{-1}(P')$ $(f(1_R) = 1_{R'} \notin P')$. We know that P is an ideal of R by Proposition 3.2.10 i). Let now $ab \in P$. Then $f(ab) = f(a)f(b) \in P'$, and since P' is prime, we have that $f(a) \in P'$ or $f(b) \in P'$. So we have $a \in P$ or $b \in P$.
ii) We know that P' is an ideal of R' by Proposition 3.2.10 ii). Moreover, $P' \neq R'$, because if $1_{R'} \in P'$, then there exists $x \in P$ such that $f(x) = f(1_R) = 1_{R'}$. But then $x - 1 \in Ker(f) \subseteq P$, so $1_R \in P$, a contradiction. Let now $a'b' \in P'$. Then $a' = f(a)$ and $b' = f(b)$, where $a, b \in R$, and $f(a)f(b) = f(ab) \in P'$. This means that $f(ab) = f(x)$ for some $x \in P$. But then $ab - x \in P$, so $ab \in P$. It follows that $a \in P$ or $b \in P$, i.e. $a' = f(a) \in f(P) = P'$, or $b' = f(b) \in f(P) = P'$. ∎

Corollary 3.4.4 *The following are equivalent for an ideal P of R:*
i) P is prime.
ii) R/P is a domain.

Proof: Use Proposition 3.4.3 for $can : R \longrightarrow R/P$, $can(x) = x + P$, $P = Ker(can)$, and $P' = \{0_{R/P}\}$. ∎

Remark 3.4.5 *We can also prove Corollary 3.4.4 using the definition of a prime ideal.*

Definition 3.4.6 *An ideal M of the commutative ring R is said to be* maximal *if $M \neq R$ and for any ideal I of R such that $M \subseteq I \subseteq R$ it follows that $I = M$ or $I = R$.*

Remark 3.4.7 *We have that $\{0_R\}$ is a maximal ideal if and only if R is a field.*

Proposition 3.4.8 *Let $f : R \longrightarrow R'$ be a surjective ring morphism (recall that all rings are commutative).*
i) If M' is a maximal ideal of R', then $M = f^{-1}(M')$ is a maximal ideal of R.
ii) If M is a maximal ideal of R such that $Ker(f) \subseteq M$, then $M' = f(M)$ is a maximal ideal of R'.

Proof: Recall that there is a bijective correspondence between the ideals of R' and the ideals of R that contain $Ker(f)$. Since this correspondence preserves inclusions, the result follows. ∎

Use Proposition 3.4.8 to prove the following:

Corollary 3.4.9 *The following are equivalent for an ideal M of R:*
i) M is maximal.
ii) R/M is a field.

Proof: Let $can : R \longrightarrow R/M$ denote the canonical surjection.
i) $\Rightarrow$ ii). We have that $M = Ker(can)$, so if M is maximal we get that $can(M) = \{M\} = \{0_{R/M}\}$ is also maximal, i.e. R/M is a field.
ii) $\Rightarrow$ i). If R/M is a field, then $\{0_{R/M}\}$ is maximal, so $M = Ker(can)$ is maximal. ∎

Remark 3.4.10 *We can also prove Corollary 3.4.9 using the definition of a maximal ideal.*

Remark 3.4.11 *i) M is a maximal ideal of $\mathbb{Z}$ if and only if $M = p\mathbb{Z}$, where p is prime.*
ii) If M is a maximal ideal of R, then M is prime.

3.5 Lecture 3.5: Polynomial rings, 1

Recall that all rings are commutative, even if the constructions in this section may be performed without this condition. If R is a ring, we recall that $R^{\mathbb{N}}$ is the set of all functions from $\mathbb{N}$ to R. If f is such a function, we can refer to it as a sequence: $f = (a_0, a_1, \ldots, a_n, \ldots)$, where $a_n = f(n)$ for all $n \in \mathbb{N}$. Since $(R, +)$ is an abelian group, we recall from Exercise 2.1.5 xix) that $R^{\mathbb{N}}$ is an abelian group with the following operation. If $f = (a_0, a_1, \ldots, a_n, \ldots)$ and $g = (b_0, b_1, \ldots, b_n, \ldots)$, then

$$f + g = (a_0 + b_0, a_1 + b_1, \ldots, a_n + b_n, \ldots).$$

Also recall that the zero element is $(0_R, 0_R, \ldots)$, and the opposite of the function $(a_0, a_1, \ldots)$ is $(-a_0, -a_1, \ldots)$. We will introduce a new operation on $R^{\mathbb{N}}$.

Proposition 3.5.1 *If $f = (a_0, a_1, \ldots, a_n, \ldots)$ and $g = (b_0, b_1, \ldots, b_n, \ldots)$, then*

$$fg = (c_0, c_1, \ldots, c_n, \ldots), \quad c_n = \sum_{i+j=n} a_i b_j, \quad n \in \mathbb{N}$$

is commutative, associative, distributive with respect to addition, and has identity element $(1_R, 0_R, 0_R, \ldots)$.

Proof: This multiplication is obviously commutative, because the multiplication in R is commutative. Let

$$h = (c_0, c_1, \ldots), \ (fg)h = (d_0, d_1, \ldots, d_n, \ldots),$$

and

$$f(gh) = (e_0, e_1, \ldots, e_n, \ldots).$$

We have

$$\begin{aligned} d_n &= \sum_{k+l=n}(\sum_{i+j=k} a_i b_j)c_l \\ &= \sum_{k+l=n}\sum_{i+j=k}(a_i b_j)c_l \\ &= \sum_{i+j+l=n}(a_i b_j)c_l \\ &= \sum_{i+j+l=n} a_i(b_j c_l) \\ &= \sum_{i+k=n}\sum_{j+l=k} a_i(b_j c_l) \\ &= \sum_{i+k=n} a_i(\sum_{j+l=k} b_j c_l) \\ &= e_n \end{aligned}$$

for all $n \in \mathbb{N}$, so the multiplication is associative. Now

$$\begin{aligned} f(g+h) &= (a_0(b_0+c_0), \ldots, \sum_{i+j=n} a_i(b_j+c_j), \ldots) \\ &= (a_0b_0 + a_0c_0, \ldots, \sum_{i+j=n} a_i b_j + \sum_{i+j=n} a_i c_j, \ldots) \\ &= fg + fh, \end{aligned}$$

so multiplication is distributive with respect to addition.
It is easy to see that $(1_R, 0_R, 0_R, \ldots)$ is the identity element for multiplication (writing the element on position j as $\delta_{0,j}$ will make this even easier).
∎

Definition 3.5.2 $(R^{\mathbb{N}}, +, \cdot)$ *is a commutative ring. If we denote*

$$X = (0_R, 1_R, 0_R, \ldots) \tag{3.1}$$

(i.e. $X : \mathbb{N} \longrightarrow R$ is the function that sends 1 to 1_R and all the other natural numbers to 0_R), then we can check that

$$X^n = (0_R, \ldots, 0_R, 1_R, 0_R, \ldots), \ \ n \text{ times } 0_R \text{ in the beginning,}$$

and an element $f = (a_0, a_1, \ldots, a_n, \ldots)$ can be written as

$$f = \sum_{i=0}^{\infty} a_i X^i,$$

where $X^0 = 1_R$. We will call f a formal series *(or formal power series), and the elements a_i the* coefficients *of the series f. We call a_0 the* free term *or the* constant term *of f. We will denote*

$$R[[X]] = R^{\mathbb{N}},$$

and we will call it the ring of formal series in one indeterminate with coefficients in R. *We will call the injective ring morphism*

$$\varphi : R \longrightarrow R[[X]], \;\; \varphi(a) = (a, 0_R, \ldots)$$

the canonical injection.

Exercise 3.5.3 *Check that the canonical injection*

$$\varphi : R \longrightarrow R[[X]], \;\; \varphi(a) = (a, 0_R, \ldots)$$

is an injective ring morphism.

Solution: We have $\varphi(a+b) = (a+b, 0_R, \ldots) = (a, 0_R, \ldots) + (b, 0_R, \ldots) = \varphi(a) + \varphi(b)$, and $\varphi(ab) = (ab, 0_R, \ldots) = (a, 0_R, \ldots)(b, 0_R, \ldots) = \varphi(a)\varphi(b)$. It is also clear that $\varphi(1_R) = (1_R, 0_R, \ldots) = 1_{R[[X]]}$, and $Ker(\varphi) = \{0_R\}$, so φ is injective.

Remark 3.5.4 *Note that it does not make much sense to call X a "variable" (even though you might see it called this way in some texts), because it does not vary, it does not take any values. In fact, X is a function defined on $\mathbb{N}$ with values in R, and its definition is given in (3.1).*

Definition 3.5.5 *A formal series with only finitely many nonzero coefficients is called a* polynomial. *The sum and product of two polynomials are also polynomials, so the polynomials form a subring of $R[[X]]$, denoted by $R[X]$. It is clear that the canonical injection φ takes values in $R[X]$. If we identify 0_R by $\varphi(0_R)$ and 1_R by $\varphi(1_R)$, then $0_{R[X]} = 0_R$ and $1_{R[X]} = 1_R$. We call $R[X]$ the* polynomial ring in one indeterminate with coefficients in R. *Note that $R[X]$ always comes with $\varphi : R \longrightarrow R[X]$, which gives a way of regarding elements of R as polynomials (called* constants*).*

Exercise 3.5.6 *Check that $R[X]$ is a subring of $R[[X]]$.*

Solution: Clearly $(1_R, 0_R, \ldots) \in R[X]$. If $f, g \in R[X]$, assume that the coefficients of X^k in f and g are zero for $k \geq n$. Then the coefficient of X^k in $f + g$ is zero for $k \geq n$, and the coefficient of X^k in fg is zero for $k \geq 2n$.

A polynomial $f \in R[X]$ may be written uniquely as

$$f = a_0 + a_1 X + a_2 X^2 + \ldots a_n X^n,$$

where $a_iX^i = \varphi(a_i)X^i = (0_R, \ldots, 0_R, a_i, 0_R, \ldots)$, i times 0_R in the beginning.

Exercise 3.5.7 *Why are the coefficients of a polynomial unique?*

Solution: A polynomial is a function defined on $\mathbb{N}$ with values in the ring R. The coefficients of the polynomial are the values of the function.

3.6 Lecture 3.6: Polynomial rings, 2

A polynomial of the form aX^i is called a *monomial.* A formal series is a formal sum of monomials, and a polynomial is a (finite) sum of monomials.

Definition 3.6.1 *If $f \in R[X]$, $f \neq 0_R$, then f may be written uniquely as*

$$f = a_0 + a_1X + a_2X^2 + \dots a_nX^n,\ a_n \neq 0_R.$$

We call n the degree *of f, and we write $deg(f) = n$ (in this case a_n is called the* leading coefficient *of f). Note that the zero polynomial does not have a degree.*

Remark 3.6.2 *Let $f, g \in R[X]$, $f, g \neq 0_R$. Then, if $f+g$ and fg are nonzero, we have:*
i) $deg(f+g) \leq max\{deg(f), deg(g)\}$. Can you give an example when we have = and an example when we have <?
ii) $deg(fg) \leq deg(f) + deg(g)$. Can you give an example when we have = and an example when we have <?

Proposition 3.6.3 *$f \in R[X]$ is a zero divisor if and only if there exists $a \in R$, $a \neq 0_R$ such that $af = 0_R$.*

Proof: Let $f = a_0 + a_1X + \ldots + a_nX^n$. Assume that $fg = 0_R$, $g \neq 0_R$, $deg(g) = m$ and m is the least possible. If $g = b_0 + b_1X + \ldots + b_mX^m$, then $a_nb_m = 0_R$, and since $f(a_ng) = 0_R$ it follows that $a_ng = 0_R$ by the minimality of m. We now write $0_R = fg = a_nX^ng + a_{n-1}X^{n-1}g + \ldots + a_1Xg + a_0g$, and since $a_ng = 0_R$, we get $a_{n-1}b_m = 0_R$, and so again $a_{n-1}g = 0_R$ by the minimality of m. We continue until we get $a_ig = 0_R$ for $i = 0, \ldots, n$, which means $b_mf = 0_R$, i.e. $m = 0$. The converse implication is obvious. ∎

Exercise 3.6.4 *i) Find the zero divisors of degree 2 in $\mathbb{Z}_6[X]$.*
ii) If R is a domain, then $R[X]$ is a domain.

Solution: i) If $f = aX^2 + bX + c \in \mathbb{Z}_6$, $a \neq 0$, is a zero divisor, by Proposition 3.6.3 there is a $d \neq 0$ in $\mathbb{Z}_6$ such that $ad = bd = cd = 0$. If $d = 2$ or $d = 4$, we have that $a = 3$, b is 0 or 3, and c is 0 or 3, so in this case we have $1 \cdot 2 \cdot 2 = 4$ polynomials: $3X^2$,$3X^2 + 3$, $3X^2 + 3X$, and $3X^2 + 3X + 3$. If $d = 3$ we have that a is 2 or 4, b is 0 or 2 or 4, and c is 0 or 2 or 4, so in this case we have $2 \cdot 3 \cdot 3 = 18$ polynomials: $2X^2$, $2X^2 + 2$, $2X^2+4$, $2X^2+2X$, $2X^2+2X+2$, $2X^2+2X+4$, $2X^2+4X$, $2X^2+4X+2$, $2X^2+4X+4$, $4X^2$, $4X^2+2$, $4X^2+4$, $4X^2+2X$, $4X^2+2X+2$, $4X^2+2X+4$,

$4X^2+4X$, $4X^2+4X+2$, and $4X^2+4X+4$.
ii) This is easy, it does not require the use of Proposition 3.6.3: if f and g are nonzero polynomials, $a_n \neq 0_R$ and $b_m \neq 0_R$ are their respective leading coefficients, then $a_n b_m \neq 0_R$ is the leading coefficient of fg.

Proposition 3.6.5 *An element $a \in R$ is called* nilpotent *if there exists $n \in \mathbb{N}$ such that $a^n = 0_R$. The set of nilpotent elements in R is an ideal, called the* nilradical *of R, and denoted by $\mathcal{N}(R)$. We have that $f \in R[X]$ is nilpotent if and only if all its coefficients are nilpotent.*

Proof: Let $f = a_0 + a_1X + \ldots + a_nX^n$. Assume that $a_i \in \mathcal{N}(R) \subseteq \mathcal{N}(R[X])$ for $0 \leq i \leq n$. Then $a_iX^i \in \mathcal{N}(R[X])$, so $f = \sum_{i=0}^{n} a_iX^i \in \mathcal{N}(R[X])$. Conversely, assume $f \in \mathcal{N}(R[X])$, $f^k = 0_R$. Then the leading coefficient of f^k is $a_n^k = 0_R$. So $a_n \in \mathcal{N}(R) \subseteq \mathcal{N}(R[X])$, and therefore $a_nX^n \in \mathcal{N}(R[X])$. Thus $f - a_nX^n \in \mathcal{N}(R[X])$, and we can continue until we get $a_0 \in \mathcal{N}(R)$. ∎

Exercise 3.6.6 *Find the nilpotents of degree 1 in $\mathbb{Z}_{12}[X]$.*

Solution: It is easy to see that if $a \in \mathbb{Z}_{12}$ is nilpotent, then a has to be divisible by both 2 and 3, so 6 and 0 are the only nilpotent elements in $\mathbb{Z}_{12}$. By Proposition 3.6.5, a nilpotent polynomial of degree 1 in $\mathbb{Z}_{12}[X]$ is of the form $aX + b$, where a, b are nilpotent and $a \neq 0$. By ii) we get that $a = 6$ and $b = 0$ or $b = 6$. In conclusion, there are two nilpotent polynomials of degree 1 in $\mathbb{Z}_{12}[X]$: $6X$ and $6X + 6$.

Proposition 3.6.7 *If u is a unit and x is nilpotent, then $u + x$ is a unit. We have that $f \in R[X]$ is a unit if and only the constant term a_0 is a unit in R and the other coefficients are nilpotent.*

Proof: Since $u + x = u(1 + u^{-1}x)$ and $u^{-1}x$ is nilpotent, we can assume $u = 1$. If $x^n = 0$, then $1 = 1 - (-x)^n = (1 + x)(1 - x + \ldots + (-x)^{n-1})$ so $1 + x$ is a unit.
Now let $f = a_0 + a_1X + \ldots + a_nX^n$. Assume that $a_0 \in U(R)$ and $a_i \in \mathcal{N}(R)$ for $1 \leq i \leq n$. We have that $a_iX^i \in \mathcal{N}(R[X])$ and $a_0 \in U(R) \subseteq U(R[X])$, so by i) $f \in U(R[X])$. Conversely, let $g = b_0 + b_1X + \ldots + b_mX^m$, $fg = 1_R$. We have $a_0b_0 = 1_R$, so $a_0 \in U(R)$. Then $a_nb_m = 0_R$ and $a_nb_{m-1} + a_{n_1}b_m = 0_R$. Multiplying the second equality by a_n and using the first, we get $a_n^2 b_{m-1} = 0_R$. We continue until we get $a_n^{m+1}b_0 = 0_R$, and since b_0 is a unit we get that a_n is nilpotent. Now a_nX^n is also nilpotent, so $a_0 + a_1X + \ldots + a_{n-1}X^{n-1} = f - a_nX^n$ is a unit by i). We continue as before until we get that $a_{n-1}, \ldots, a_1$ are nilpotent. ∎

Exercise 3.6.8 *Find the units of degree 1 in $\mathbb{Z}_{12}[X]$.*

Solution: By Proposition 3.6.7, a unit of degree 1 is of the form $aX + b$, where $b \in \mathbf{U}_{12} = \{1, 5, 7, 11\}$ and $a \neq 0$ is nilpotent, i.e. $a = 6$. In conclusion, there are four units of degree one in $\mathbb{Z}_{12}[X]$: $6X + 1$, $6X + 5$, $6X + 7$, and $6X + 11$.

Like the factor set, the factor group, and the factor ring, the polynomial ring also satisfies a universal property.

Theorem 3.6.9 *Let R be a commutative ring, $R[X]$ the polynomial ring, and $\varphi : R \longrightarrow R[X]$ the canonical injection. Then for any commutative ring A, any ring morphism $\psi : R \longrightarrow A$, and any $x \in A$, there exists a unique ring morphism $\theta : R[X] \longrightarrow A$ such that $\theta(X) = x$ and $\theta\varphi = \psi$, i.e. such that the diagram*

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[dr, "\psi"'] & R[X] \arrow[d, "\theta"] \\ & A \end{tikzcd}$$

is commutative.

Exercise 3.6.10 *Prove Theorem 3.6.9.*
(Hint: If $f \in R[X]$, $f = \sum_{i=0}^{n} a_i X^i = \sum_{i=0}^{n} \varphi(a_i) X^i$, put $\theta(f) = \sum_{i=0}^{n} \psi(a_i) x^i$.)

The universal property may be used to produce new examples of rings. If we take $R = \mathbb{Z}$, $A = \mathbb{C}$, $\psi : \mathbb{Z} \longrightarrow \mathbb{C}$ the inclusion, and $x = i$, we denote $Im(\theta)$ by $\mathbb{Z}[i]$, and call it the ring of Gauss integers. Using the fact that $i^2 = -1$, we have

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}.$$

Now take $R = \mathbb{Z}$, $A = \mathbb{C}$, $\psi : \mathbb{Z} \longrightarrow \mathbb{C}$ the inclusion, and $x = i\sqrt{3}$. We denote $Im(\theta)$ by $\mathbb{Z}[i\sqrt{3}]$. Using the fact that $(i\sqrt{3})^2 = -3$, we have

$$\mathbb{Z}[i\sqrt{3}] = \{a + bi\sqrt{3} \mid a, b \in \mathbb{Z}\}.$$

If we take $R = \mathbb{Z}$, $A = \mathbb{R}$, $\psi : \mathbb{Z} \longrightarrow \mathbb{R}$ the inclusion, and $x = \sqrt{2}$, we denote $Im(\theta)$ by $\mathbb{Z}[\sqrt{2}]$. Using the fact that $(\sqrt{2})^2 = 2$, we have

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}.$$

Another application of the universal property is the definition of a polynomial function. If $a \in R$, by the universal property there exists a ring morphism $\theta : R[X] \longrightarrow R$ such that $\theta(X) = a$. If $f \in R[X]$, we will denote $\theta(f)$ by $f(a)$ (when we do this we say that we specialize X to a). In this way, the polynomial f defines a function $\tilde{f} : R \longrightarrow R$, $\tilde{f}(x) = f(x)$ for $x \in R$. If $f = a_0 + a_1 X + a_2 X^2 + \ldots a_n X^n$, we have that

$$\tilde{f}(x) = f(x) = a_0 + a_1 x + a_2 x^2 + \ldots a_n x^n.$$

Note that in this notation, x is a variable, it can be any element of R. For polynomial functions, unlike polynomials, it is no longer true that if $\tilde{f} = 0_R$ (the constant function 0_R) then all coefficients are also equal to zero. An example is the polynomial function associated to the polynomial $f = X^2 + X \in \mathbb{Z}_2[X]$. The associated function is $\tilde{f} : \mathbb{Z}_2 \longrightarrow \mathbb{Z}_2$, $\tilde{f}(x) = x^2 + x$ for $x \in \mathbb{Z}_2$. Then $\tilde{f}(0) = 0^2 + 0 = 0$, and $\tilde{f}(1) = 1^2 + 1 = 1 + 1 = 0$, so $\tilde{f} = 0$, even though $f \neq 0$. As we will see later (look after Exercise 3.7.6), this cannot happen if R is an infinite domain. Note that in general f is a function from $\mathbb{N}$ to R, while $\tilde{f}$ is a function from R to R (or from A to A, where A is a ring to which we have a ring morphism from R). Sometimes the polynomial functions are called simply polynomials. For example, the "polynomials" studied in high school are in fact polynomial functions.

3.7 Lecture 3.7: Polynomial rings, 3

Theorem 3.7.1 *i) Let K be a field, and $f, g \in K[X]$, $g \neq 0$. There exist $q, r \in K[X]$ such that $f = qg + r$, where $r = 0$ or $\deg(r) < \deg(g)$.*
ii) Let K be a field, and $f, g \in K[[X]]$, $g \neq 0$. There exist $q, r \in K[[X]]$ such that $f = qg + r$, where $r = 0$ or $\mathrm{ord}(r) < \mathrm{ord}(g)$.

Proof: i) The proof is similar to the one of Theorem 1.3.1. If $g \mid f$, then $f = qg$ for some $q \in K[X]$, and we take $r = 0$. If $g \nmid f$ (note that this implies that $f \neq 0$), we let $W = \{\deg(f - eg) \mid e \in K[X]\}$. By the well-ordering principle, we let $r = f - qg$ such that $\deg(r)$ is a least element of W. We want to show that $\deg(r) < \deg(g)$. If $\deg(r) = \deg(f - qg) = n \geq m = \deg(g)$, we write $r = f - qg = aX^n + a_{n-1}X^{n-1} + \ldots$ and $g = bX^m + b_{m-1}X^{m-1} + \ldots$. Then $f - qg - ab^{-1}X^{n-m}g$ has degree less than $\deg(r)$, a contradiction.
ii) The proof is identical to the proof of i), except we write $r = f - qg = aX^n + a_{n+1}X^{n+1} + \ldots$ and $g = bX^m + b_{m+1}X^{m+1} + \ldots$, and we replace degree by order everywhere.
We remark that the proofs of i) and ii) above are exactly the long division algorithms for polynomials and power series as you have seen them in beginning algebra and calculus. ∎

Remark 3.7.2 *We remark that the conclusion of Theorem 3.7.1 remains true for polynomials with coefficients in an arbitrary domain if the leading coefficient of g is a unit.*

Exercise 3.7.3 *Show that q and r from the statement of Theorem 3.7.1 are unique.*

Solution: Assume $f = q_1g + r_1 = q_2g + r_2$. If $r_1 \neq r_2$, then $g(q_1 - q_2) = r_2 - r_1$, and $deg(g) < deg(r_2 - r_1)$, a contradiction. It follows that $r_1 = r_2$, so $q_1 = q_2$ as well, because $K[X]$ is a domain and $g \neq 0$. For the formal series case, just replace degree by order.

Corollary 3.7.4 (Bézout's Little Theorem) *Let R be a domain, and $a \in R$. For any $f \in R[X]$, the remainder of f when divided by $X - a$ is $f(a)$ (the value of the polynomial function defined by f at $a \in R$). Consequently, $X - a \mid f$ if and only if $f(a) = 0$ (we say that a is a* root *of f).*

Proof: By Theorem 3.7.1 and Remark 3.7.2, we have that $f = (X-a)q+r$, where $r \in R$. After specializing X at a we get that $f(a) = r$. ∎

Exercise 3.7.5 (Rational Root Theorem) *If $\frac{a}{b} \in \mathbb{Q}$, $(a, b) = 1$, is a root of*

$$f = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 \in \mathbb{Z}[X],$$

then $a \mid a_0$ and $b \mid a_n$.

Exercise 3.7.6 *If R is a domain and $f \in R[X]$ is a non-zero polynomial, then f has at most n roots, where $n = \deg(f)$. Is this true if R is not a domain?*

Solution: Induction on n. If $n = 0$, then $0 \neq f \in R$, so f has no roots. If $n \geq 1$ and f has a root a, then $f = (X - a)g$, where $deg(g) = n - 1$ by Corollary 3.7.4. By the induction hypothesis g has at most $n - 1$ roots, so f has at most $n - 1 + 1 = n$ roots.

The assertion is false if R is not a domain, the polynomial $2X \in \mathbb{Z}_4[X]$ has degree one and two roots, 0 and 2.

The previous exercise shows that if R is an infinite domain, we cannot have two different polynomials defining the same polynomial function. Indeed, the difference of the two polynomials would then have infinitely many roots, which is not possible, the number of roots is bounded by the degree. This is the reason why we can get away with identifying polynomials with polynomial functions in high school mathematics.

Exercise 3.7.7 *Let $p \in \mathbb{Z}$ be prime. Use the polynomial $(X - 1) \cdots (X - p + 1) - X^{p-1} + 1 \in \mathbb{Z}_p[X]$ to give another proof for Wilson's Theorem: $(p - 1)! \equiv -1$ (mod p) (see Exercise 3.3.8).*

Solution: Assume $p > 2$. By Fermat's Little Theorem (Exercise 3.3.7 viii)), f has roots 1, 2, $\ldots, p - 1$. Since it has degree at most $p - 2$, by Exercise 3.7.6 it follows that $f = 0$. Specializing X at 0 gives $(p-1)! \equiv -1$ (mod p).

Definition 3.7.8 *A complex number $\alpha \in \mathbb{C}$ is called* algebraic *over the subfield $K \subseteq \mathbb{C}$ if α is the root of a polynomial in $K[X]$.*

Proposition 3.7.9 *An algebraic number α is a root for a unique monic polynomial in $K[X]$ which is called the* minimal polynomial *of α over K. The* degree *of α is $deg(Irr(\alpha, K))$.*

Proof: By the well-ordering principle we choose a polynomial f with minimal degree among all polynomials in $K[X]$ that have α as a root. If $g \in K[X]$ and $g(\alpha) = 0$, we write $g = qf + r$, where $r = 0$ or $deg(r) < deg(f)$. Since $r(\alpha) = 0$, we have that $r = 0$, otherwise the minimality of $deg(f)$ would be contradicted. It follows that any polynomial that has α as a root and has the same degree as f is associated in divisibility with f, i.e. it is equal to af for some $a \in K$, $a \neq 0$. There is only one monic polynomial associated in divisibility with f, and that is $Irr(\alpha, K)$. ∎

Definition 3.7.10 *The* splitting field *of a polynomial $f \in K[X]$ is the smallest subfield of $\mathbb{C}$ containing K and all the roots of f. The* degree *of the splitting field is the minimum number of elements in it such that all the other elements in the splitting field can be written as linear combinations (with coefficients in K) of them.*

3.8 Lecture 3.8: Rings of fractions

Recall that all rings considered here are commutative.

Definition 3.8.1 *Let R be a commutative ring, and $S \subseteq R$. We say that S is a* multiplicative subset *if the following conditions are satisfied:*
MS1) $1_R \in S$.
MS2) if $s, t \in S$, then $st \in S$.
MS3) S does not contain any zero divisors.

Remarks 3.8.2 *i) If P is a prime ideal of R, show then $R \setminus P$ has properties MS1) and MS2): $1_R \notin P$ because $P \neq R$. If $a \notin P$ and $b \notin P$, then $ab \notin P$ by the definition of a prime ideal.*
ii) If R is a domain and P is a prime ideal of R, then $R \setminus P$ is a multiplicative set. This follows from i) and the fact that there are no zero divisors in R.
iii) If R is a domain, then $S = R^* = \{r \in R \mid r \neq 0_R\}$ is a multiplicative set. This follows from ii), because $\{0_R\}$ is a prime ideal in R.
iv) If $f \in R$ is not a zero divisor, then $S = \{f^k \mid k \in \mathbb{N}\}$ is a multiplicative set: $1_R = f^0 \in S$. If $k, l \in \mathbb{N}$, then $f^k f^l = f^{k+l} \in S$. If $f^k a = f f^{k-1} a = 0_R$, then $f^{k-1} a = 0_R$ since f is not a zero divisor, and we can continue until we get $a = 0_R$.
v) If R is a commutative ring, the set $S = \{s \in R \mid s \text{ is not a zero divisor}\}$ is a multiplicative subset: 1_R is not a zero divisor. It is clear that if a, b are not zero divisors, then ab is not a zero divisor.
vi) $\{1, 3, 5\} \subseteq \mathbb{Z}_6$ is not a multiplicative set, because 3 is a zero divisor.
vii) $\{1, 3, 5, 7\} \subseteq \mathbb{Z}_8$ is a multiplicative set, because it is the set of units in $\mathbb{Z}_8$.

Lemma 3.8.3 *Let R be a commutative ring and S a multiplicative subset in R. The relation on $R \times S$ defined by*

$$(a, s) \sim (b, t) \ \Leftrightarrow at = bs$$

is an equivalence relation.

Proof: The relation is clearly reflexive, i.e. for any $(a, s) \in R \times S$ we have $(a, s) \sim (a, s)$, since $as = as$. If $(a, s) \sim (b, t)$, then $at = bs$, so $bs = at$, and therefore $(b, t) \sim (a, s)$, i.e. the relation is symmetric. Finally, if $(a, s) \sim (b, t)$ and $(b, t) \sim (c, u)$, then $at = bs$ and $bu = ct$. Multiplying the first equality by u and the second one by s, we get $atu = bsu$, and $bsu = cts$. Consequently, we get $atu = cts$, so $t(au - cs) = 0_R$. Since $t \in S$ is not a zero divisor, we get $au = cs$, i.e. $(a, s) = (c, u)$, so the relation is transitive, and the proof is complete. ∎

The equivalence class of the element $(a, s) \in R \times S$ will be denoted by $\dfrac{a}{s}$ and called a *fraction*. The element a will be called the *numerator* of the fraction $\dfrac{a}{s}$, and the element s will be called the denominator of the fraction $\dfrac{a}{s}$. We remark that if we allow zero divisors in S, then the relation defined in Lemma 3.8.3 is not an equivalence relation, because it is not transitive. To see this, assume that $a \in S$ and $b \in R$, $b \neq 0_R$ such that $ab = 0_R$. Then we have

$$\frac{b}{1_R} = \frac{ab}{a} = \frac{0_R}{a} = \frac{0_R}{1_R},$$

since it is easy to check each equality, however $\dfrac{b}{1_R} \neq \dfrac{0_R}{1_R}$, because $b \neq 0_R$. It is possible to allow zero divisors in S by changing the definition of the equivalence relation on $R \times S$, but we will not do this here.

Proposition 3.8.4 *Let R be a commutative ring, S a multiplicative subset in R, and denote by*

$$S^{-1}R = \frac{R \times S}{\sim} = \left\{ \frac{a}{s} \mid (a, s) \in R \times S \right\}$$

the factor set of the set $R \times S$ relative to the equivalence relation $\sim$. Then $S^{-1}R$ becomes a commutative ring with the following operations:

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st},$$

and

$$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}.$$

Moreover, the map

$$\varphi_S : R \longrightarrow S^{-1}R, \;\; \varphi(a) = \frac{a}{1_R}$$

is an injective ring morphism that sends each $s \in S$ to a unit in $S^{-1}R$. We will call φ_S the canonical injection*.*

Proof: We first need to show that the two operations are well defined, i.e. the definitions do not depend on the representatives chosen. This means that if $\dfrac{a}{s} = \dfrac{a'}{s'}$ and $\dfrac{b}{t} = \dfrac{b'}{t'}$, we need to prove that

$$\frac{at + bs}{st} = \frac{a't' + b's'}{s't'},$$

and

$$\frac{ab}{st} = \frac{a'b'}{s't'}.$$

In order to prove the first equality, we need to show that $(at + bs)s't' = (a't'+b's')st$. We know that $as' = a's$ and $bt' = b't$, so, after multiplying the first by tt' and the second by ss', we get $ats't' = a't'st$ and $bss't' = b's'st$, which can be added to obtain the desired equality.
In order to prove the second equality, we need to show that $abs't' = a'b'st$, which can be obtained by multiplying $as' = a's$ and $bt' = b't$.
It may be immediately checked that the addition of fractions defined above is associative and commutative. Then we have that $0_{S^{-1}R} = \frac{0_R}{1_R} = \frac{0_R}{s}$ for any $s \in S$, and the opposite of $\frac{a}{s}$ is $\frac{-a}{s}$, so $S^{-1}R$ is an abelian group with $+$.
The multiplication of fractions is obviously associative and commutative, and $1_{S^{-1}R} = \frac{1_R}{1_R} = \frac{s}{s}$ for any $s \in S$. Distributivity is also easy to check, so $S^{-1}R$ is a commutative ring.
It is obvious that φ_S is a ring morphism, and if $\frac{a}{1_R} = \frac{0_R}{1_R}$, then $a = 0_R$, i.e. $Ker(\varphi_S) = \{0_R\}$, so φ_S is injective.
Finally, if $s \in S$, then $\varphi(s) = \frac{s}{1_R}$ is a unit with inverse $(\varphi(s))^{-1} = \frac{1_R}{s}$. ▮

Definition 3.8.5 *We will call the pair $(S^{-1}R, \varphi_S)$, defined in Proposition 3.8.4, the* ring of fractions *of R relative to S (or with denominators in S).*

The ring of fractions has the following universal property:

Theorem 3.8.6 (The Universal Property of the Ring of Fractions) *Let R be a commutative ring, S a multiplicative subset in R, and $(S^{-1}R, \varphi_S)$ the ring of fractions of the ring R with denominators in S. Then for any commutative ring A, and any ring morphism $\psi : R \longrightarrow A$, with the property that $\psi(s)$ is a unit in A for any $s \in S$, there exists a unique ring morphism $\theta : S^{-1}R \longrightarrow A$ such that $\psi = \theta\varphi_S$, which means that the diagram*

$$\begin{tikzcd}
R \arrow[r, "\varphi_S"] \arrow[dr, "\psi"'] & S^{-1}R \arrow[d, "\theta"] \\
& A
\end{tikzcd}$$

is commutative.

Proof: Define $\theta\left(\frac{a}{s}\right) = \psi(a)\psi(s)^{-1}$. The definition is correct, because if $\frac{a}{s} = \frac{a'}{s'}$, then $as' = a's$, so $\psi(as') = \psi(a's)$, or $\psi(a)\psi(s') = \psi(a')\psi(s)$, and so, after multiplying by $\psi(s)^{-1}\psi(s')^{-1}$ we get $\psi(a)\psi(s)^{-1} = \psi(a')\psi(s')^{-1}$. We check that θ is a ring morphism:

$$\begin{aligned}
\theta\left(\frac{a}{s}+\frac{b}{t}\right) &= \theta\left(\frac{at+bs}{st}\right)\\
&= \psi(at+bs)\psi(st)^{-1}\\
&= (\psi(at)+\psi(bs))\psi(s)^{-1}\psi(t)^{-1}\\
&= \psi(a)\psi(t)\psi(t)^{-1}\psi(s)^{-1}+\psi(b)\psi(s)\psi(s)^{-1}\psi(t)^{-1}\\
&= \psi(a)\psi(s)^{-1}+\psi(b)\psi(t)^{-1}\\
&= \theta\left(\frac{a}{s}\right)+\theta\left(\frac{b}{t}\right),
\end{aligned}$$

$$\begin{aligned}
\theta\left(\frac{a}{s}\cdot\frac{b}{t}\right) &= \theta\left(\frac{ab}{st}\right)\\
&= \psi(ab)\psi(st)^{-1}\\
&= \psi(a)\psi(b)\psi(s)^{-1}\psi(t)^{-1}\\
&= \psi(a)\psi(s)^{-1}\psi(b)\psi(t)^{-1}\\
&= \theta\left(\frac{a}{s}\right)\theta\left(\frac{b}{t}\right),
\end{aligned}$$

and

$$\theta\left(\frac{1_R}{1_R}\right) = \psi(1_R)\psi(1_R)^{-1} = 1_X 1_X = 1_X.$$

We have that

$$\theta(\varphi_S(a)) = \theta\left(\frac{a}{1_R}\right) = \psi(a)\psi(1_R)^{-1} = \psi(a)1_X = \psi(a),$$

so $\psi = \theta\varphi_S$.
We now show that θ is unique. If θ' is another morphism with the property

that $\psi = \theta'\varphi_S$, we have

$$\begin{aligned}\theta'\left(\frac{a}{s}\right) &= \theta'\left(\frac{a}{1_R}\right)\theta'\left(\frac{1_R}{s}\right)\\ &= \theta'\left(\frac{a}{1_R}\right)\theta'\left(\frac{s}{1_R}\right)^{-1}\\ &= \theta'(\varphi_S(a))\theta'(\varphi_S(s))^{-1}\\ &= \psi(a)\psi(s)^{-1}\\ &= \theta\left(\frac{a}{s}\right).\end{aligned}$$

∎

The following corollary says that the ring of fractions is unique, up to an isomorphism, among the rings satisfying the same universal property.

Corollary 3.8.7 *If the pair (T, ξ), where $\xi : R \longrightarrow T$ sends the elements of S to units in T, satisfies the universal property in Theorem 3.8.6, then there exists an isomorphism $\theta : S^{-1}R \longrightarrow T$ such that $\theta\varphi_S = \xi$, i.e. the diagram*

$$\begin{tikzcd} R \arrow[r, "\varphi_S"] \arrow[dr, "\xi"'] & S^{-1}R \arrow[d, "\theta"] \\ & T \end{tikzcd}$$

is commutative.

Proof: By the universal property for $(S^{-1}R, \varphi_S)$ there exists a ring morphism $\theta : S^{-1}R \longrightarrow T$ such that $\theta\varphi_S = \xi$, and by the universal property for (T, ξ) there exists a ring morphism $\theta' : T \longrightarrow S^{-1}R$ such that $\theta'\xi = \varphi_S$. It follows that $\theta'\theta\varphi_S = \theta'\xi = \varphi_S$, and $\theta\theta'\xi = \theta\varphi_S = \xi$. Since we also have that $Id_{S^{-1}R}\varphi_S = \varphi_S$ and $Id_T\xi = \xi$, by the uniqueness of the morphism in the universal property we get that $\theta\theta' = Id_T$ and $\theta'\theta = Id_{S^{-1}R}$, i.e. θ and θ' are isomorphisms inverse to each other. ∎

Definition 3.8.8 *If R is a domain, P is a prime ideal of R, and $S = R\backslash P$, the ring of fractions $(S^{-1}R, \varphi_S)$ is denoted by (R_P, φ_P), and is called the* localization *of R at the prime ideal P.*

We will refer to the ring of fractions $(S^{-1}R, \varphi_S)$ simply as $S^{-1}R$, with the understanding that it always comes with the injective ring morphism $\varphi_S : R \longrightarrow S^{-1}R$, $\varphi(a) = \dfrac{a}{1_R}$.

Definition 3.8.9 *If S is the multiplicative subset of Remarks 3.8.2 v), then we will call the ring of fractions $S^{-1}R$ the* total ring of fractions *of the ring R.*

Example 3.8.10 *The total ring of fractions of a domain R is a field, called the* field of fractions *of the domain R. Because of Definition 3.8.8, the field of fractions of the domain R is sometimes denoted by $R_{\{0_R\}}$. If $\dfrac{a}{b} \neq \dfrac{0_R}{1_R}$, it follows that $a \neq 0_R$, so $\left(\dfrac{a}{b}\right)^{-1} = \dfrac{b}{a}$.*

Index