Math 531 (Modern Algebra) Notes

Pramana Saldin

Spring 2022

University of Wisconsin-Milwaukee's Modern Algebra class for undergraduates/graduates. Integers; groups; rings; fields; emphasis on proofs. Professor: Burns Healy. Book: Abstract Algebra by John A. Beachy and William D. Blair (4rd Edition).

Contents

§1 Semester 1

§1.1 CHAPTER 1: Integers

The integers are defined as:

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

We can use elementary number theory to determine when cycles repeat, for example,

Example 1.1. $i^k = i^j \iff j - k \mid 4.$

Example 1.2.

$$\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2} i.$$

$\omega^k = \omega^j \iff j - k \mid 3.$

Math research is like a ball. We inflate it as we discover new things, so there is more surface area on the outside to discover even *more* things.

§1.2 Divisors

$\mathbb{N}$ is used for $\{1, 2, \ldots\}$.

Definition 1.3. a is a multiple of b if

$$a = qb, \ q \in \mathbb{Z}.$$

Also b divides a is written as $b \mid a$.

Set of all multiples of a is denoted $a\mathbb{Z}$. The only multiple of 0 is 0. If $b \mid a$, then $|b| \leq |a|$. Therefore if $b \mid 1$, then $b = \pm 1$.

Axiom 1.4 (Well-Ordering Principle)

Any set of natural numbers has contains a smallest element.

Theorem 1.5 (The Division Algorithm)

For any integers a, b with $b > 0$, there exist *unique* q and r such that:

$$a = bq + r \text{ with } 0 \leq r < b.$$

Proof. Solving for r gives us

$$r = a - bq$$

Consider the set

$$R = \{a - bq \mid q \in \mathbb{Z}\}.$$

First we show that R^+, the set of positive values in R, is non-empty. $a-b(-|a|) = a + b \cdot |a|$ is in the set and is non-negative since $b \geq 1$.

Now to show that $0 \leq r < b$, suppose some $s \geq b$ exists and we let $s = r - b$. Then

$$s = a - b(q+1) \in R^+,$$

but $s < r$, contradicting our definition.

And finally, we prove q and r are unique by supposing they arent: $a = bp + s$, which implies $|s - r| < b$.

$$bp + s = bq + r \implies s - r = b(q - p) \implies b \mid s - r.$$

But then since $|s - r| < b$, $s - r = 0$. ☐

Theorem 1.6

Let I be a nonempty set of integers closed under addition and subtraction. Either $I = \{0\}$ or the smallest element of I generates the rest.

Proof. We first show the set contains a positive element to apply the well ordering principle. One of $a, -a \in I$ is positive.

Claim 1.7 — $I = b\mathbb{Z}$

$b\mathbb{Z} \subseteq I$ because I is closed under addition and therefore contains all multiples of b.

To show $I \subseteq b\mathbb{Z}$, we write an element $c \in I$ as $c = bq + r$ by division algorithm. Since I contains bq, it must contain $r = c - bq$. But this is a contradiction unless $r = 0$, since b was chosen as the smallest element. We conclude $r = 0$, and $I = b\mathbb{Z}$. ☐

Definition 1.8 (Greatest Common Divisor)**.** Denoted $d = (a, b)$. d must be divisible by a and b, and any shared divisor of a and b must divide d.

Theorem 1.9

If $d = (a, b)$, then the smallest linear combination of a and b evaluates to d. Moreover, an integer is a linear combination of a and b iff it has divisor d.

Proof. We show that the set generated by linear combinations of a and b easily, omitted. By 1.6, all we need to show is that the smallest element of linear combinations of a and b is d. First we show $1.d \mid a, d \mid b$, which is clear, since $a, b \in I$. Secondly, if $c \mid a$ and $c \mid b$, then

$$d = ma + nb = m(cq_1) + n(cq_2) = c(mq_1 + nq_2),$$

completing our proof. ☐

We introduce the **Euclidean Algorithm**, which uses the fact that when $a = bq + r$, $(a, b) = (b, r)$.

Example 1.10. $(24, 18) = (18, 6) = 6$.

We can also do it with matrices to find linear combinations that add to a number :D.

§1.3 Primes

Proposition 1.11

$(a, b) = 1 \iff$ there is a linear combination of a and b that sums to 1.

Proof. Both ways follow from 1.9. □

Proposition 1.12

If $a, b, c \in \mathbb{Z}$ and $a = 0$ *or* $b = 0$,

1. $b \mid ac \implies b \mid (a, b) \cdot c$.
2. $b \mid ac$ and $(a, b) = 1 \implies b \mid c$.
3. $b \mid a, c \mid a$, and $(b, c) = 1$, then $bc \mid a$.
4. $(a, bc) = 1 \iff (a, b) = 1$ and $(a, c) = 1$.

Proof. (1.) Represent (a, b) as $ma + nb$. Then

$$(a, b) \cdot c = mac + mnb.$$

First term is divisible by b from the assumption, second term is divisible by b.
(2.) Follows from (1)
(3.) $a = bq$, and therefore, $c \mid bq$. It follows from (2) that $c \mid q$ or $q = cp$. Then $a = bcp$.
(4.) If $(a, bc) = 1$, then $ma + nbc = 1$, so we factor out b and c from the second term, completing our proof. Converse: Add linear combinations that sum to 1 and factor. □

Lemma 1.13 (Euclid's Lemma)

$p > 1$ is prime if and only if it satisfies: for all integers a, b, if $p \mid ab$, the either $p \mid a$ or $p \mid b$.

Proof. We know that $(p, a) = p$ or 1. Finish from there. Converse: Assume p is composite and derive contradiction. □

Corollary 1.14 (Last one but generalized)
$p \mid a_1 a_2 \cdots a_n \iff p \mid a_i$ for all $1 \leq i \leq n$.

Theorem 1.15 (Fundamental Theorem of Arithmetic)
Every integer a can be factorized *uniquely* as the product of prime factors.

Proof. Suppose b is the smallest integer that cannot be factored. If it was prime it could be factorizable, so it is composite. Then $b = cd$. But then c, d are factorizable and then b is too.

To prove uniqueness: Suppose a is the smallest integer that has 2 unique factorizations. 1.14 says that each prime divisor is equal. Now suppose

$$s = \frac{a}{p_1} = \frac{a}{q_1}.$$

Either $s = 1$, which implies a has a unique factorization, or $s > 1$, which implies s has 2 factorizations, but since $s < a$, we have a contradiction! □

Definition 1.16. Least common multiple of a and b, denoted $m = [a, b]$ if m is a multiple of both a and b, and any other multiple of the two is a multiple of m.

We can see that

$$(a, b) \cdot [a, b] = ab.$$

§1.4 Congruences

Definition 1.17. $a \equiv b \bmod n$ is congruence.

Proposition 1.18
Let $n > 0$ be an integer.

1. $a \equiv c \bmod n$ and $b \equiv d \bmod n$, then $a \pm b \equiv c \pm d \bmod n$ and multiplication too
2. If $a + c \equiv a + d \bmod n$, then $c \equiv d \bmod n$. If $ac \equiv ad \bmod n$, and $(a, n) = 1$, then $c \equiv d \bmod n$.

Proof. (1.) Addition/subtraction is obvious.

Since $n \mid (a - c)$, $n \mid (ab - cb)$, and $n \mid (c - d) \implies n \mid (cb - cd)$. We add those to get

$$n \mid ab - cb + cb - cd \implies n \mid ab - cd.$$

So $ab \equiv cd \bmod n$.

(2.) Addition is again obvious by subtracting the two equations.

$ac \equiv ad \implies n \mid (ac - ad)$. From 1.12, $(a, c) = 1$ lets us skip to $n \mid c - d$, from which follows $c \equiv d \bmod n$. □

Proposition 1.19

NT; if $a, n > 1$ are integers, there exists an integer b such that $ab \equiv 1 \bmod n$ if and only if $(a, n) = 1$.

Proof. If we assume that $ab \equiv 1 \bmod n$, then $ab = qn + 1$, but then some linear combination of a and n has sum 1. Therefore, $(a, n) = 1$.

Converse: We know that a linear combination exists, therefore we finish. □

Theorem 1.20

Let a, b and $n > 1$ be integers. The congruence $ax \equiv b \bmod n$ has a solution if and only if b is divisible by d, where $d = (a, n)$.

If $d \mid b$, then there are d distinct solutions $\mod n$ and these solutions are congruent $\mod \frac{n}{d}$.

Proof. For the first statement, we know that $as = b + nq$, and then we see a linear combination of a and n to b. This is a bijection.

For the second, we know that $d \mid b$ because of the properties of (a, n). Let $m = \frac{n}{d}$. If x_1 and x_2 are solutions, then $ax_1 \equiv ax_2 \bmod n$. Therefore, $n \mid a(x_2 - x_1)$. But then $n \mid d(x_2 - x_1)$, and $m \mid (x_2 - x_1)$. It follows that $x_2 \equiv x_1 \bmod m$. Easily follows the other way.

Given any of the n solutions, we can add m and be find the others, giving d distinct solutions. □

The book introduces a way to calculate linear congruences.

$$ax \equiv b \bmod n$$

First we compute $d = (a, n)$, and there are solutions if $d \mid b$. We then divide the equation by d.

$$a_1 x \equiv b_1 \bmod n_1.$$

We now know that a_1 and n_1 are relatively prime, then we can use the Euclidean Algorithm to find them.

We then try to find c that satisdy

$$ca_1 \equiv 1 \pmod m$$

Example 1.21 (Homogeneous Linear Congruences). We try to find the solutions to

$$ax \equiv 0 \bmod n.$$

The first step is to find integers such that $a_1 x \equiv 0 \bmod n_1$. But since $(a_1, n_1) = 1$, we can cancel, giving us:

$$x \equiv 0 \bmod n, \qquad \text{such that: } n_1 = \frac{n}{(a, n)}$$

Example-example: $28x \equiv 0 \bmod 48$ reduces to $x \equiv 0 \bmod 12$. The solutions are $0, 12, 24, 36$ modulo 48.

Theorem 1.22 (Chinese Remainder Theorem)
Given that $(n, m) = 1$:

$$x \equiv a \bmod n \qquad y \equiv b \bmod m,$$

has a solution, and all solutions are equivalent modulo mn.

Proof. Given that $(n, m) = 1$, then we can write $rm + sn = 1$. We let $x = arm + bsn$, and direct computations verify that this x satisfies the original system. Last part is true because they must be equal mod both of them. □

§1.5 Integers modulo n

Example 1.23. Elements of $\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$

Make sure to use the proper square bracket notations! We usually let a number be a **representative** of the congruence class. For example, $[5]_3 = [8]_3$. It's best to choose one that is less than n, so $[2]_3$.

Proposition 1.24

Addition and multiplication is well-defined in congruence classes. In symbols,

$$[a]_n + [b]_n = [a+b]_n \qquad [a]_n \cdot [b]_n = [ab]_n.$$

Proof. We need to show our choices a and b do not matter, just what congruence class they represent. Let x and y be congruent to a and b respectively $\bmod n$, so they represent the same congruence classes. Therefore we just need to prove that addition and multiplication is well defined modulo n, which it is. □

Definition 1.25. If $[a]_n \in \mathbb{Z}_n$ and $[a]_n[b]_n = [0]_n$ for some nonzero congruence class $[b]_n$, then $[a]_n$ is called a **divisor of zero**.

Definition 1.26. If $[a]_n$ has a multiplicative inverse, then we call it a **unit** of $\mathbb{Z}_n$.

Proposition 1.27

$[a]_n$ is a unit if and only if $(a, n) = 1$. A non-zero element of $\mathbb{Z}_n$ either has a multiplicative inverse or is a divisor of zero.

Example 1.28 (Finding Multiplicative Inverses). $[11]_{16}^{-1}$ can be found by the Euclidean Algorithm. It evaluates to $[3]_{16}$.

Proposition 1.29

Euler's φ function can be calculated for $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ as

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

Definition 1.30. The set of units of $\mathbb{Z}_n$ $[a]$ such that $(a, n) = 1$ is denoted $\mathbb{Z}_n^\times$.

Note that $\mathbb{Z}_n^\times$ is closed under multiplication.

Theorem 1.31 (Euler)
If $(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Proof. There are $\varphi(n)$ congruence classes, $\{a_1, a_2, \ldots, a_{\varphi(n)}\}$. When we multiply all of them by a, they are all still unique, so they represent the same classes.

$$a_1 a_2 \cdots a_{\varphi(n)} = (aa_1)(aa_2) \cdots (aa_{\varphi(n)}) = a^{\varphi(n)} a_1 a_2 \cdots a_{\varphi(n)}$$

Therefore by cancelling:

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

□

Corollary 1.32 (Fermat)
p is prime $\implies a^p \equiv a \pmod{n}$.

Proof. If $p \mid a$ we are done. Otherwise use $\varphi(p) = p - 1$ if p prime and finish. □

§1.6 Chapter 1 End Remarks

- Lagrange proved in 1770 that every positive integer can be expressed as the sum of 4 squares.
- Gauss proved in 1801 that all n that are not in the form $4^m(8k+7)$ with $m, k \in \mathbb{Z}^*$ can be expressed as the sum of 3 squares.
- Finally, Euler proved in 1749 that n can be expressed as the sum of 2 squares if and only if when we factor n as a product of primes, the numbers that are congruent to 3 modulo 4 have even exponents.

§1.7 CHAPTER 2: Functions

One-to-one correspondences are important. $\mathbb{Z}_5^\times$ is the same as $\mathbb{Z}_4$ pretty much, if only there was a name for that...

§1.8 Functions

Introduce $\mathbb{R}, \mathbb{Q}, \mathbb{C}$.

Definition 1.33. Given $F : S \to T$, F is a subset of $S \times T$ such that for each element $x \in S$, there is exactly one element $y \in T$ such that $(x, y) \in F$.
S is the **domain**, and T is the **codomain**. The subset

$$\{y \in T \mid (x, y) \in F \text{ for some } x \in S\}$$

of the codomain is called the **image** of f.

Example 1.34. Given that $S = \{1, 2, 3\}$ and $T = \{4, 5, 6\}$. We can assign F (called the **graph**)

$$F = \{(1, 4), (2, 5), (3, 6)\}$$

and

$$F = \{(1, 4), (2, 4), (3, 4)\}$$

and are functions, but

$$F = \{(1, 4), (2, 5), (2, 6)\}$$

is not unless we change S to $\{1, 3\}$

We also use the notation $f : S \to T$, and use $\text{Im}_{f(S)}$ to represent the image.

Example 1.35 (Inclusion Function)**.** If $A \subseteq T$, $\iota : A \to T$ is called the **inclusion function**. Graph of ι is

$$I = \{(x, x) \in A \times T \mid x \in A\}$$

Sometimes a function is not **well-defined**.

Example 1.36. $f : \mathbb{Q} \to \mathbb{Z}$ is defined as

$$f(m/n) = m.$$

However, $f(1/2) = 1$ and $f(3/6) = 3$, but the inputs are equal, so it is not well-defined.

All we need to show that a function f is well-defined is that $x_1 = x_2 \implies f(x_1) = f(x_2)$.

Definition 1.37. Composite of functions $f : S \to T$ and $g : T \to U$ is denoted $(g \circ f)(x)$. Rigorous definition is

$$\{(x, z) \mid (x, y) \in F \text{ and } (y, z) \in G \text{ for some } y \in T\}$$

Definition 1.38. For a function $f : S \to T$, it is
Surjective if for any element $y \in T$, there is some $x \in S$.
Injective if $f(x_1) = f(x_2) \implies x_1 = x_2$.
Bijective if both.

Note that $f : S \to T$ is onto if Im_f is equal to the codomain T.

Example 1.39. Let $f : S \to T$ be a function. Define $\hat{f} : F \to f(S)$ by $\hat{f}(x) = f(x)$ for all $x \in S$. By definition $\hat{f}$ is surjective. If $\iota : f(S) \to T$ is the inclusion function, then $f = \iota \circ \hat{f}$, and we have written f as the composite of surjective function and a injective function.

Proposition 1.40

a. If f and g are injective, then $f \circ g$ and $g \circ f$ is injective.
b. If f and g are surjective, then $f \circ g$ and $g \circ f$ is surjective.

a. Let $g(f(x_1)) = g(f(x_2))$ and finish each using injective definition.
b. There is always something that we can find in the composition of the two so then each must be surjective. (rough sketch, rewrite?)

Definition 1.41. A function is an **identity** if everything maps to itself. A function is an **inverse** if composition of each in both directions results in identities. In symbols, given $f : S \to T$ and $g : T \to S$:

$$g \circ f = 1_S \text{ and } f \circ g = 1_T.$$

Proposition 1.42

$f : S \to T$ is a function. f has an inverse $\iff$ f is bijective. Inverse is also unique.

Proof. Assume f has inverse g. Then by definitions, $g \circ f = 1_S$ and $f \circ g = 1_T$. Given any element $y \in T$, we have

$$y = 1_T(y) = f(g(y)),$$

and so f maps $g(y)$ onto y. f is surjective. To show f is injective, let $f(x_1) = f(x_2)$, then $g(f(x_1)) = g(f(x_2))$, then we must have $x_1 = x_2$ because the composition is the identity function.

Conversely if f is injective and surjective, we define $g : T \to S$ as follows. For each $y \in T$, there exists an element $x \in S$ with $f(x) = y$. Furthermore, there is one such $x \in S$ such that f is injective.

We then define $g(y) = x$, and it follows that $g(f(x)) = x$ for all $x \in S$.

To establish uniqueness, suppose that $h : T \to S$ is also an inverse of f. Then

$$h = h \circ 1_T = h(fg) = (hf)g = 1_S \circ g = g,$$

as desired. □

Proposition 1.43

Let $f : S \to T$ where both S and T are finite with the same number of elements. Then f is bijective if either f is injective or surjective.

Proof. Suppose $|S| = |T| = n$. If f is injective, then

$$B = \{f(x_1), f(x_2), \dots f(x_n)\} \subseteq T,$$

it is easy to see with the fact that f is injective that $B = T$, so f is surjective.

If f is surjective, then suppose that some $f(z) = f(z') = y_i$ where $z \neq z'$. Consider the subset

$$A = \{z, z', z_1 \dots, z_{i-1}, z_{i+1}, \dots, z_n\} \subseteq S.$$

But this is impossible since A has more elements than S. Therefore f is also injective. □

§1.9 Equivalence Relations

Definition 1.44. The **equivalence relation** is a subset R of $S \times S$ such that

1. For all $a \in S$ $(a, a) \in R$. - reflexive
2. $(a, b) \in R \implies (b, a) \in R$. - symmetric
3. $(a, b), (b, c) \in R \implies (a, c) \in R$. - transitive

Definition 1.45. $S/\sim$ is the set of all equivalence classes, called the **factor set**.

Example 1.46. The factor set of S determined by $f : S \to T$ is denoted S/f. We will see later that the function $\overline{f} : S/f \to T$ is a injective function.

Proposition 1.47

Each element of a set S belongs to exactly one equivalence class of S determined by $\sim$.

Proof. Suppose that $a \in [a], [b]$. We wish to show that $[a] = [b]$. Suppose that some $x \in [a]$, use equivalence properties and finish. □

Definition 1.48. $\mathcal{P}$ is a partition of S if it splits it up (very rigorous terms I know).

Proposition 1.49

Any partition $\mathcal{P}$ of S determines a unique equivalence relation on S such that $\mathcal{P} = S/\sim$.

Conversely, $S/\sim$ is a partition that determines the equivalence relation $\sim$.

Proof. $\mathcal{P}$ follows equivalence relations well.

$\mathcal{P}$ has element P_a. We can show that $P_a = [a]$ by showing that each is a subset of the other. Therefore $\mathcal{P} \subseteq S/\sim$.

Let $[a] \in S/\sim$. Let P_a be a unique element of $\mathcal{P}$ for which $a \in P_a$. We show that $[a]$ and P_a are subsets of each other. Therefore $[a] = P_a \in \mathcal{P}$, so $\mathcal{P} = S/\sim$.

Clearly the equivalence relation partitions the group from 1.47.

To prove that equivalence relation partitions are unique, suppose we have another one $\sim_2$. If $a, b \in S$ and same equivalence class $[a] \in S/\sim$, then we have $a \sim_2 b$. Conversely, if $a \sim_2 b$, then we pick an element in their equivalence class and use transitivity to show that $a \sim b$. Therefore $a \sim b \iff a \sim_2 b$, so they are the same. □

Example 1.50. The function $\psi : S \to S/\sim$ defined by $\psi(x) = [x]$ is a **natural projection** from S onto its factor set $S/\sim$.

Theorem 1.51

If $f : S \to T$ is any function, and $\sim_f$ is an equivalence relation that says $x_1 \sim_f x_2$ if $f(x_1) = f(x_2)$, then there is a bijection between the elements of the image of $f(S)$ and the equivalence classes of S/f.

Proof. Use the function $\overline{f} : S/f \to F(S)$ by $\overline{f}([x]) = f(x)$. It is easy to prove $\overline{f}$ is well defined and that it is bijective. □

We can turn a function f in "better behaving" functions. We let ψ be an inclusion mapping, π be a natural projection, and $\overline{f}$ be defined from the last theorem.

$$S \xhookrightarrow{\pi} S/f \xrightarrow{\overline{f}} f(S) \xrightarrow{\psi} T$$

Notably, π is surjective, $\overline{f}$ is bijective, and ψ is injective.

Definition 1.52. If $f : S \to T$ is a function and $B \subseteq T$, then the set

$$\{x \in S \mid f(x) \in B\}$$

is called the **inverse image** of B under f.

We sometimes use the notation $f^{-1}(B)$, which may be confused with the inverse function.

Example 1.53. We can write the inverse image of any element of the image of f with its corresponding equivalence class.

$$S/f = \{f^{-1}(y) \mid y \in f(S)\}.$$

Note that when f is bijective, we know that each inverse image represents a single element. Therefore the notation kinda makes sense.

§1.10 Permutations

Definition 1.54. All bijections of a set S to itself are **permutations**. The set of all permutations of S is denoted $\mathrm{Sym}(S)$. The set of all permutations of $\{1, 2, \ldots, n\}$ is S_n.

S_n has $n!$ elements. To invert σ, simply switch the top and bottom rows of the permutation and sort the top.

Example 1.55. Given

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix},$$

then

$$\sigma^{-1} = \begin{pmatrix} 4 & 3 & 1 & 2 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$$

Introduction to cycles here...

Example 1.56.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix},$$

can be written as $(1, 4, 2, 3)$.

Proposition 1.57

Two disjoint cycles σ, τ commute.

Proof. (sketch) if we compose both, anything that is affected by σ remains fixed by τ and vice versa. If some element is in neither than it is fixed by both, nice. □

Theorem 1.58

Every permutation of S_n can be written as the product of disjoint cycles.

Proof. There is some minimum r such that σ^r sends 1 to 1. Then we have distinct cycles

$$(1, \sigma(1), \dots \sigma^{r-1}(1))$$

If $r < n$, then let a be the least integer not in the set. Continue creating cycles like this. We have developed an algorithm for creating disjoint cycles. □

This is similar for doing composition of cycles, just make sure you do it right to left.

Example 1.59. Given cycles

$$(2, 5, 1, 4, 3) \text{ and } (4, 6, 2),$$

first we run 1 through it. It gets sent to 4, which gets sent to 6, then to 5.
Then 2 gets sent to 3, and we finish since we have covered all. Therefore

$$(2, 5, 1, 4, 3)(4, 6, 2) = (1, 4, 6, 5)(2, 3).$$

Definition 1.60. The order m of a permutation σ such that $\sigma^m = (1)$.

Proposition 1.61

If σ has order m and $\sigma^i = \sigma^j \iff i \equiv j \bmod m$.

Proposition 1.62

If σ is written as the product of disjoint cycles, then its order is the lcm of the cycle lengths.

The inverse of a cycle is as simple as reversing the order of the cycle.

Definition 1.63. A cycle of length 2 is called a **transposition**.

Proposition 1.64

Any permutation can be written as the product of transpositions.

Theorem 1.65

You cannot express an even permutation as an odd one, and vice-versa.

Proof. Suppose you can. Then write

$$\sigma = a_1 a_2 \cdots a_{2m} = b_1 b_2 \cdots b_{2n+1}.$$

Therefore

$$(1) = \sigma\sigma^{-1} = a_1 a_2 \cdots a_{2m} b_{2n+1} b_{2n} \cdots b_1,$$

and note that we have written (1) as an odd permutation.

Next suppose that $(1) = p_1 p_2 \cdots p_k$ is the shortest odd permutation of σ. Also suppose that $p_1 = (a, b)$. But then a must appear somewhere else in a transposition, otherwise $p_1 p_2 \cdots p_k(a) = b$, contradiction. Assume that our product has the least number of a's.

Let (a, u, v, r) be distinct. Then $(u, v)(a, r) = (a, r)(u, v)$, and $(u, v)(a, v) = (a, u)(u, v)$. Therefore we can move a to the next transposition. Let the next transposition with a be $p_2 = (a, c)$. If $c = b$, then $p_1 p_2 = (1)$ and $p_3 p_4 \cdots p_k = (1)$, which is shorter, contradiction.

Otherwise, since $(a, b)(a, c) = (a, c)(b, c)$, so $(1) = (a, c)(b, c) p_3 p_4 \cdots p_k$, but it has fewer a's. Another contradiction. □

§1.11 CHAPTER 3: Groups

Introduces binary operations, the idea of associativity, identity and inverses. In fact, the binary operation has at most one identity element, and each element has at most one inverse.

§1.12 Definition of a Group

Proposition 1.66

For a binary operation and $a, b \in S$,

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

Definition 1.67. Groups satisfy 4 properties (the first is a result of binary operations). **Closure** (For all $a, b \in G$, the element $a * b$ is well-defined element of G), **Associativity, Identity, Inverses**.

Example 1.68. $\mathbb{R}^\times, \mathbb{Q}^\times, \mathbb{C}^\times$ are all groups. $\mathbb{Z}^\times$ is a group if its only elements are ± 1.

Proposition 1.69

If $a, b \in G$ where G is a group, then each of the equations $ax = b$ and $xa = b$ have unique solutions.

Conversely if G is a nonempty set with a binary operation so $ax = b$ and $xa = b$ have solutions $\forall a, b \in G$, then G is a group.

Definition 1.70 (Niels Abel)**.** Commutative groups are called **abelian**.

Order of a group, if $|G|$ not finite, it is infinite.

Example 1.71. The set of units of $\mathbb{Z}_n^\times$ is an abelian group.

Example 1.72. $\mathrm{GL}_n(\mathbb{R})$ is a group. Don't forget the 2×2 matrix inverse:

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

§1.13 Subgroups

H is a subgroup if it is subset of G and is a group under the operation used by G (*induced*).

Example 1.73. $\mathrm{SL}_n(\mathbb{R}) \leq \mathrm{GL}_n(\mathbb{R})$.

Proposition 1.74 (Subgroup Properties)
$H \leq G$ if and only if:

1. $ab \in H\ \forall a, b \in H$.
2. $e \in H$.
3. $a^{-1} \in H\ \forall a \in H$.

Corollary 1.75 (One Step Subgroup Test)
$H \leq G$ iff H nonempty and $ab^{-1} \in H\ \forall a, b \in H$.

Corollary 1.76
If H is a *finite* nonempty subset of a group G, then $H \leq G \iff ab \in H\ \forall a, b \in H$.

Proposition 1.77
Let G be a group with $a \in G$.

- $\langle a \rangle \leq G$.
- Any $K \leq G$ with $a \in K \implies \langle a \rangle \subseteq K$.

Intersection of subgroups is a subgroup. **Cyclic groups** are $\langle a \rangle$. $\mathbb{Z}$ has generator 1 or -1.

Lemma 1.78
Let $H \leq G$. For $a, b \in G$, define $a \sim b$ if $ab^{-1} \in H$. Then $\sim$ is an equivalence relation.

Proof. Reflexive: $aa^{-1} = e \in H$. Symmetric: $ab^{-1} \in H$ but then $(ab^{-1})^{-1} \in H$. Transitive: $(ab^{-1})(bc^{-1}) = ab^{-1} \in H$. □

Theorem 1.79 (Lagrange's Theorem)
The order of any subgroup is a divisor of $|G|$.

Let $|G| = n, |H| = m$. Use $\sim$ from the last lemma.

Claim 1.80 — For any $a \in G$, the function $p_a : H \to [a]$, $x \mapsto xa\ \forall x \in H$ is a bijection between H and $[a]$.

Im_f is correct since $p_a(h) = ha \in [a]$ and $(ha)(a^{-1}) = h \in H$. p_a injective because $ha = ka$ simplifies to $h = k$ by group cancellation. p_o surjective since if $y \in G$ with $y \sim a$, then $ya^{-1} = h$ for some $h \in H$, and thus $p_a(x) = y$ has a solution $x = h$. $ha = (ya^{-1})a = y$.

Therefore each equivalence class has m elements, and it partitions G equally, so $n = mt$.

Corollary 1.81

Any group of prime order is cyclic.

§1.14 Constructing Examples

There can be multiple groups of a certain order. For example $\mathbb{Z}_6$ has order 6, and so does

$$S_3 = \{e, a, a^2, b, ab, a^2b \mid a^3 = e, b^2 = e, ba = a^2b\},$$

where $a = (1, 2, 3), b = (1, 2)$.

Definition 1.82. Suppose that $S, T \subseteq G$, where G is a group. Then the **set-theoretic product** of S, T is defined as

$$ST := \{x \in G \mid x = st, s \in S, t \in T\}.$$

Same applies for subgroups.

Proposition 1.83

Let G be a group with $H, K \leq G$. If $h^{-1}kh \in K \forall h \in H, k \in K$, then $HK \leq G$.

Proposition 1.84 (Direct Product Groups)

Operation for product of groups is

$$(a, b)(c, d) = (ac, bd).$$

If $a_1 \in G_1$ and $a_2 \in G_2$ have orders m, n respectively, then $(a_1, a_2) \in G_1 \times G_2$ has order $[m, n]$.

Example 1.85. Klein four-group is $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Example 1.86. $\mathbb{Z}_2 \times \mathbb{Z}_3$ is cyclic, but $\mathbb{Z}_2 \times \mathbb{Z}_4$ is not.

Proposition 1.87

Let F be field. Then $\mathrm{GL}_n(F)$ is a group under matrix multiplication.

Proof. Suppose A, B are invertible matrices. Then $(A^{-1})^{-1} = A$ and $(AB)^{-1} = B^{-1}A^{-1}$ hold, meaning that elements have inverses, and is closed under matrix multiplication. □

Example 1.88. $\mathrm{GL}_2(\mathbb{C})$ is the **quaternion group**, where

$$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, i = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} j = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} k = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}.$$

We verify that $i^2 = j^2 = k^2 = -1$, and $ij = k, jk = i, ki = j$. This group is not abelion nor cyclic, as $|-1| = 2$, but $|\pm i| = |\pm j| = |\pm k| = 4$ ($|g|$ means the order of g, not the absolute value).

Definition 1.89. If $S \subseteq G$ with S nonempty, a finite product of elements of S and their inverses is called a **word** in S. The set of all words is denoted $\langle S \rangle$.

Proposition 1.90

If $S \subseteq G$ and nonempty, then $\langle S \rangle \leq G$, and is the intersection of all groups that contain S.

§1.15 Isomorphisms

If there is a bijection between elements of groups and operations are preserved (i.e. $\phi(a*b) = \phi(a)\cdot\phi(b)$), we call that an **isomorphism**. ϕ *must* be bijective.

Proposition 1.91

The inverse of a group isomorphism is a group isomorphism. The compostion of two group isomorphisms is a group isomorphism.

Proposition 1.92

Let $\phi : G_1 \to G_2$ be an ismorphism. If $a \in G$ has order n, then $|\phi(a)| = n$. If G_1 abelian or cyclic, then so is G_2.

Example 1.93. $\mathbb{R} \ncong \mathbb{R}^\times$, since $|-1| = 2$ in $\mathbb{R}^\times$, but the only value that satisfies $2x = 0$ in $\mathbb{R}$ is $x = 0$, the identity.

Proposition 1.94

Let $\phi : G_1 \to G_2$ be a function such that $\phi(ab) = \phi(a)\phi(b)$. ϕ is injective $\iff \phi(x) = e \implies x = e \forall x \in G_1$.

§1.16 Cyclic Groups

Theorem 1.95

Every subgroup of a cyclic group is cyclic.

Proof. (sketch) Find smallest element, s. Claim: the subgroup is generated by s. Use the fact that $k = mq + r$ with k being the smallest power that could be the order of s. □

Corollary 1.96

If $m, k \mid n$, then $\langle a^m \rangle \subseteq \langle a^k \rangle \iff k \mid m$.

Proof. Suppose that $k \mid m \implies m = kq$, then $a^m = (a^k)^q \in \langle a^k \rangle$. Therefore $\langle a^m \rangle \subseteq \langle a^k \rangle$.

Conversely, assume $\langle a^m \rangle \subseteq \langle a^k \rangle \implies a^m \in \langle a^k \rangle \implies m \equiv kt \pmod{n}$ for $t \in \mathbb{Z}$. It follows that $m = kt + nq$ for some $q \in \mathbb{Z}$, so $k \mid m$. □

The notation $m\mathbb{Z}_n$ will be used for the subgroup $\langle [m] \rangle$ in $\mathbb{Z}_n$.

Theorem 1.97 (Finite Cyclic Group Structure Theorem)

If $n = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$

$$\mathbb{Z}_n \cong \bigtimes_{i=1}^{n} \mathbb{Z}_{p_i^{a_i}}.$$

Definition 1.98. $\exists N$ for a group G such that $a^N = e \forall a \in G$. The smallest such N is called the **exponent** of G.

Lemma 1.99

If $a, b \in G$ with $ab = ba$, and the orders of a, b are relatively prime, then $o(ab) = o(a)o(b)$.

Proof. Let $o(a) = n, o(b) = m$, then $(ab)^{mn} = a^{mn}b^{mn} = e$. Therefore ab has finite order. If that order is k, then $k \mid mn$. $(ab)^k = e \implies a^k = b^{-k}$. So $a^{km} = (b^m)^{-k} = e$, so $n \mid km$. Since $(n, m) = 1$, we have $n \mid k$. A similar argument shows that $m \mid k$, then $mn \mid k$. So $k = mn$. □

Proposition 1.100

Given G is finite abelian group. Exponent of G is equal to the order of any element of G of largest order. The group G is cyclic $\iff$ its exponent is equal to its order.

§1.17 Permutation Groups

Definition 1.101. Any subgroup of the symmetric group $\mathrm{Sym}(S)$ on a set S is called a permutation group.

Theorem 1.102 (Cayley's Theorem)

Every group is isomorphic to a permutation group.

Proof. Let G be any group. Define λ_a (for $a \in G$) as

$$\lambda_a(x) = ax.$$

Then λ_a is surjective and injective, so we can conclude that it is a permutation of G. So $\phi : G \to \mathrm{Sym}(G)$ defined by $\phi(a) = \lambda_a$ is well-defined.

Next we show that

$$G_\lambda = \phi(G) \leq \mathrm{Sym}(G).$$

We first need the fact that $\lambda_a\lambda_b = \lambda_{ab}$. Also, $(\lambda_a)^{-1} = \lambda_{a^{-1}}$. This shows that G_λ is closed and has identity and inverses. So it is a subgroup.

ϕ clearly preserve products. To finish showing that $\phi : G \to G_\lambda$ is an isomorphism, we need to show that it is injective. It is surjective by definition of G_λ. It is easy to show that $\phi(a) = \phi(b) \implies a = b$ because $\lambda_a(e) = \lambda_b(e)$.

In conclusion we found that $G_\lambda \leq \mathrm{Sym}(G)$ and isomorphism $\phi : G \to G_\lambda$ defined by assigning each $a \in G$ to permutation λ_a. □

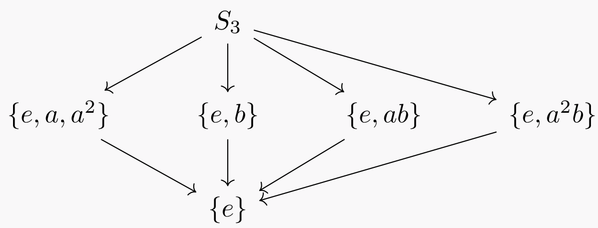
Example 1.103. The rigid motions of an equilateral triangle yield the group S_3.

Example 1.104 (General Case - Rigid Motion of n-gon)**.** Consider the set

$$S = \{a^k, a^k b \mid 0 \leq k < n, a^n = e, b^2 = e\},$$

moreover we see that $bab = a^{-1} \implies ba = a^{-1}b$.

Example 1.105. Here is a visualization of the subgroups of S_3:



Proposition 1.106

The set of all even permutations on S_n is a subgroup of S_n.

Proof. For any two permutations that are even, their product must also be even. This shows that it is closed. The identity is even, which is good. Also since S_n is finite, it is clear that it is a subgroup. □

Definition 1.107. The **alternating group** is A_n, consisting of all even permutations in S_n.

We can now use a new polynomial definition to prove that even permutations are always even and odd always odd, regardless of their presentation. Consider the polynomial

$$\Delta_n = \prod_{1 \le i < j \le n} (x_i - x_j).$$

If we let a permutation act on the the values of i, j, then the polynomial either stays the same or negates.

Theorem 1.108

A permutation $\sigma \in S_n$ is even $\iff \Delta_n = \sigma(\Delta_n)$.

Proof. Let $X = \{\Delta_n, -\Delta_n\}$. Let $\widehat{\sigma} : X \to X$ by

$$\widehat{\sigma}(\Delta_n) = \prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}),$$

and

$$\widehat{\sigma}(-\Delta_n) = -\prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

We show that any transposition $\tau = (r, s)$ has $\widehat{\tau}(\Delta_n) = -\Delta_n$. If we assume that $r < s$, this is clear by showing that the term

$$(x_{\tau(r)} - x_{\tau(s)}) = (x_s - x_r) = -(x_r - x_s).$$

Then it reduces to showing the cases $i > s$, $r < i < s$, $i < r$, which is easy to prove.

Since we can write any permutation out of transpositions, we have

$$\widehat{\sigma}(\Delta_n) = (-1)^k \Delta_n,$$

where σ can be written in k transpositions. □

§2 Semester 2

§2.1 Homomorphisms

Definition 2.1. A **homomorphism** is a function $\phi : G \to H$ such that $\phi(ab) = \phi(a)\phi(b) \forall a, b \in G$.

Proposition 2.2

Let $\phi : G_1 \to G_2$ be a homomorphism.

1. $\phi(e) = e$
2. $\phi(a^{-1}) = (\phi(a))^{-1}$
3. $\phi(a^n) = (\phi(a))^n$
4. $(|\phi(a)|) \mid a$

Example 2.3 (Parity of a Permutation). Let $G = \{\pm 1\} \leq \mathbb{Q}^\times$. $\phi : S_n \to G$ is a homomorphism defined as $\phi(\sigma) = 1$ if even permutation and $\phi(\sigma) = -1$ if odd permutation.

Definition 2.4. The **kernel** of a homomorphism ϕ, denoted $\ker(\phi)$ is all elements that map to e.

Proposition 2.5

Suppose ϕ has $K = \ker(\phi)$,

1. $K \leq G$ such that $gkg^{-1} \in K \forall k \in K, g \in G$.
2. ϕ is injective $\iff K = \{e\}$.

Definition 2.6. H is called the **normal** subgroup of G if $ghg^{-1} \in H$.

Proposition 2.7

For ϕ,

1. If $H_1 \leq G$ then $\phi(H_1) \leq G$. If ϕ is surjective and $H_1 \trianglelefteq G_1$, then $\phi(H_1) \trianglelefteq G_2$.
2. If $H_2 \leq G_2$, then

   $$\phi^{-1}(H_2) = \{x \in G \mid \phi(x) \in H_2\},$$

   is a subgroup of G. If $H_2 \trianglelefteq G_2$, then $\phi^{-1}(H_2) \trianglelefteq G_1$.

Proposition 2.8

With our homomorphism ϕ, the multiplication of equivalence classes in G_1/ϕ is well-defined, and G_1/ϕ is a group. The natural projection $\pi : G_1 \to G_1/\phi$ defined as $\pi(x) = [x]_\phi$ is a homomorphism.

Theorem 2.9

With our homomorphism $\phi : G_1 \to G_2$,

$$\overline{\phi} : G_1/\phi \to \phi(G_1),$$

with $\overline{\phi}([a]_\phi) = \phi(a)$ exists as an isomorphism.

Proof. To show ϕ is well defined and injective, notice that $[a]_\phi = [b]\phi \iff \phi(a) = \phi(b) \iff \overline{\phi}([a]_\phi) = \overline{\phi}([b]_\phi)$. The image of G_1/ϕ is

$$\{\overline{\phi}([a]_\phi) \mid a \in G_1\} = \{\phi(a) \mid a \in G_1\} = \phi(G_1).$$

so $\overline{\phi}$ is surjective. Finally, function is preserved,

$$\overline{\phi}([a]_\phi)\overline{\phi}([b]_\phi) = \phi(a)\phi(b) = \phi(ab) = \overline{\phi}([ab]_\phi) = \overline{\phi}([a]_\phi[b]_\phi).$$

□

Example 2.10 (Cayley's Theorem). Let $\phi : G \to \mathrm{Sym}(G)$ by $\phi(a) = \lambda_a$ with $\lambda_a(x) = ax \forall x \in G$. After showing that λ_a is a bijection, we can use the fact that ϕ is a homomorphism ($\lambda_a\lambda_b = \lambda_{ab}$) and the fact that λ_a is an identity permutation only if $a = e$, meaning $\ker(\phi) = \{e\}$. Thus G is isomorphic to $\phi(G)$, a permutation group.

Proposition 2.11

Let $\phi : G_1 \to G_2$ be a homomorphism with $a, b \in G_1$. All of the following statements are equivalent.

1. $\phi(a) = \phi(b)$
2. $ab^{-1} \in \ker(\phi)$
3. $\exists k \in \ker(\phi), a = kb$
4. $b^{-1}a \in \ker(\phi)$
5. $\exists k \in \ker(\phi), a = bk$.

§2.2 Cosets, Normal Subgroups, Factor Groups

Proposition 2.12

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

Corollary 2.13

If $H \leq G$, the relation $\sim$ defined on G as $a \sim b$ if $aH = bH \forall a, b \in G$ is an equivalence relation on G.

Since equivalence classes partition G, we now are able to separate the group into a bunch of sets.

Definition 2.14. For $H \leq G$ and $a \in G$,

$$aH = \{x \in G \mid x = ah \text{ for some } h \in H\},$$

is called the **left coset**; **right coset** is the other way around.

The number of left cosets of H in G is called the **index** of H in G, denoted $[G : H]$.

Additionally, $[G : H] = |G| / |H|$, since all left cosets have the same size (proof sketch: consider $f : H \to aH$, and show it is bijective).

Proposition 2.15 (Multiplication of Left Cosets is Well-Defined)

If N is normal in G, then for $a, b, c, d \in G$, $aN = cN$ and $bN = dN \implies abN = cdN$.

Proof. The statement implies $a^{-1}c \in N$ and $b^{-1}d \in N$. Since N is normal, $d^{-1}(a^{-1}c)d \in N$, but since $b^{-1}d \in N$, $(ab)^{-1}cd = (b^{-1}d)(d^{-1}a^{-1}cd) \in N$. Therefore $abN = cdN$ as desired. □

Theorem 2.16

If N is a normal subgroup of G, then the set of left cosets of N forms a group under coset multiplication:

$$aNbN = abN, \forall a, b \in G.$$

Proof. Identity is $N = eN$. The inverse of aN is $a^{-1}N$ because $aNa^{-1}N = eN$ and $a^{-1}NaN = eN$. For associativity,

$$(aNbN)cN = abNcN = (ab)cN = a(bc)N = aNbcN = aN(bNcN).$$

□

Definition 2.17. The **factor group** of G is the group of all left cosets of N, a normal subgroup to G. Denoted G/N.

Proposition 2.18

Let N be a normal subgroup of G:

1. The **natural projection** $\pi : G \to G/N$, defined as $\pi(x) = xN \forall x \in G$ is a homomorphism and $\ker(\pi) = N$.

2. There is a bijection between subgroups of G/N and subgroups H of G with $H \supseteq N$. If $K \leq G/N$, then $\pi^{-1}(K)$ is the corresponding subgroup of G. Similarly, if $H \leq G$ with $H \supseteq N$, then $\pi(H)$ is the corresponding subgroup of G/N.

Normal subgroups correspond to normal subgroups.

Proposition 2.19

Let $H \leq G$. $H \trianglelefteq G \iff aH = Ha \forall a \in G \iff \forall a, b \in G, abH$ is the set theoretic product $(aH)(bH) \iff (\forall ab^{-1} \in H \iff a^{-1}b \in H)$.

Example 2.20 (Normal Subgroups of S_3)**.** The only normal subgroup of S_3 is $\{e\}$, S_3, and $\{b, a^b, ab\}$. Proof: casework on all the other subgroups, sorry!

Subgroups of index 2 are always normal!

Theorem 2.21 (Fundamental Homomorphism Theorem)

If $\phi : G_1 \to G_2$ is a homomorphism with $K = \ker(\phi)$, then $G_1/K \cong \phi(G_1)$.

Proof. Function used: $\overline{\phi} : G_1/K \to \phi(G_1)$ by $\overline{\phi}(aK) = \phi(a)$. □

Definition 2.22. The nontrivial group G is called **simple** if it has no proper nontrivial normal subgroups.

Example 2.23. With the homomorphism $\phi : \mathbb{Z}_n \to \mathbb{Z}_m$ by $\phi([x]_n) = [x]_m$.

$$\ker(\phi) = \{[x]_n \mid [x]_m = [0]_m\} = \{[x]_n \mid x \text{ is a multiple of } m\},$$

which means that $\ker(\phi) = m\mathbb{Z}_n$. Therefore $\mathbb{Z}_n/m\mathbb{Z}_n \cong \mathbb{Z}_m$.

Anther useful takeaway involving the direct product on normal subgroups,

$$(G_1 \times G_2)/(N_1 \times N_2) \cong (G_1/N_1) \times (G_2/N_2).$$

Example 2.24. Define $\phi : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$ by $\phi(A) = \det(A)$. It is easy to prove that this is a homomorphism. $\ker(\phi)$ is $\mathrm{SL}_n(\mathbb{R})$, which is a normal subgroup. So $\mathrm{GL}_n(\mathbb{R}) / \mathrm{SL}_n(\mathbb{R}) \cong \mathbb{R}^\times$.

§2.3 Chapter 3 End Remarks

In 1870, Kronecker came up with the definition of commutative groups, and in 1893 Heinrich Weber came up with the general case.

§2.4 CHAPTER 4: Polynomials

Proofs and methods from chapter 1 involving integers can be extended into polynomials as well, and will be covered. Typically, the fields covered will be $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, and $\mathbb{Z}_p$, where p is prime.

§2.5 Fields; Roots of Polynomials

Roots are found until they are all contained in the smallest possible field E such that $\mathbb{Q} \subseteq E \subseteq \mathbb{C}$.

Definition 2.25. A field has to be **closed, associative, commutative, distributive**, have a additive/multiplicative **identity**, and additive/multiplicative **inverses**.

Proposition 2.26

For a field F,

1. $\forall a \in F, a \cdot 0 = 0$
2. $a, b \in F, a \neq 0, b \neq 0 \implies ab \neq 0$
3. $\forall a \in F, -(-a) = a$
4. $\forall a, b \in F, a(-b) = (-a)b = -ab$
5. $(-a)(-b) = ab$.

Definition 2.27. A **polynomial over** a field F is what you expect. Notable terms: **indeterminate** is x. The polynomial is **constant** if a_0 is leading coefficient. Denoted $F[x]$.

A zero polynomial ($f(x) = 0$) has degree $-\infty$.

Example 2.28 (Polynomials over $\mathbb{Z}_5$)**.** Recall by Fermat's theorem, $c^5 \equiv c \pmod 5$, so really, $f(x) = x^5$ and $g(x) = x$ are really the same.

Moreover, $x^5 - 2x + 1 \equiv -c + 1 \equiv 4c + 1 \pmod 5$.

Covers basic polynomial stuff. $f(x)g(x) = f(x)h(h) \implies g(x) = h(x)$ when $f(x) \neq 0$. **Divisor** of a polynomial is when you can write $f(x) = q(x)g(x)$ for some $q(x) \in F[x]$.

Lemma 2.29

For any element $c \in F$,

$$(x - c) \mid (x^k - c^k).$$

Proof. $(x^k - c^k) = (x - c)(x^{k-1} + cx^{k-2} + \cdots + c^{k-2}x + c^{k-1})$. □

Theorem 2.30 (Remainder Theorem)
Given $f(x) \in F[x], f(x) \neq 0$, let $c \in F$. $\exists q(x) \in F[x]$ such that

$$f(x) = q(x)(x - c) + f(c).$$

Moreover, if $f(x) = q_1(x)(x - c) + k$, where $q_1(x) \in F[x]$, and $k \in F$, then $q_1(x) = q(x)$ and $k = f(c)$.

Proof.

$$f(x) - f(c) = a_m(x^m - c^m) + \cdots + a_1(x - c).$$

But the last lemma tells us that $(x - c)$ divides all the terms, so

$$f(x) - f(c) = q(x)(x - c) \iff f(x) = q(x)(x - c) + f(c).$$

If $f(x) = q_1(x)(x - c) + k$, then

$$(q(x) - q_1(x))(x - c) = k - f(c).$$

But the RHS is constant, so $q(x) - q_1(x) = 0 \implies k - f(c) = 0$, and the quotient and remainder are unique. □

Corollary 2.31
c is a root of $f(x) \in F[x] \iff (x - c) \mid f(x)$.

Corollary 2.32
A polynomial of degree in n in the field F has at most n distinct roots in F.

§2.6 Factors

Theorem 2.33 (Division Algorithm)
For polynomials $f(x), g(x) \in F[x]$, with $g(x) \neq 0, \exists q(x), r(x) \in F[x]$ such that

$$f(x) = q(x)g(x) + r(x),$$

and either $\deg(r) < \deg(g)$ or $r(x) = 0$.

Proof. Use polynomial long division inductively. To show they are unique, let

$$f(x) = q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x),$$

$$\implies (q_1(x) - q_2(x))g(x) = r_2(x) - r_1(x).$$

When we check the degree of r_1, r_2, we find that they must be equal to the degree of $(q_1(x) - q_2(x))g(x)$, but that is contradiction, forcing us to have $q_1(x) - q_2(x) = 0$. $r_1 = r_2, q_1 = q_2$. □

Theorem 2.34

Let $I \subseteq F[x]$ such that

1. I contains nonzero polynomial
2. $f(x), g(x) \in I \implies f(x) + g(x) \in I$
3. $f(x) \in I, q(x) \in F[x] \implies q(x)f(x) \in I$.

If $d(x)$ is any nonzero polynomial in I of minimal degree, then

$$I = \{f(x) \in F[x] \mid f(x) = q(x)d(x) \text{ for some } q(x) \in F[x]\}.$$

Definition 2.35. A monic polynomial $d(x) \in F[x]$ is called the greatest common divisor of $f(x), g(x) \in F[x]$ if

1. $d(x)$ is a divisor of both $f(x)$ and $g(x)$
2. any divisor of both $f(x)$ and $g(x)$ is also a divisor of $d(x)$.

Theorem 2.36

$\gcd(f(x), g(x)) = a(x)f(x) + b(x)g(x)$ for some $a(x), b(x) \in F[x]$.

Proof.

$$I = \{a(x)f(x) + b(x)g(x) \mid a(x), b(x) \in F[x]\}$$

satisfies the conditions of the last theorem. Since $f(x), g(x) \in I$, we have $d(x) \mid f(x), g(x)$. Since $d(x)$ is some linear combination of $f(x)$ and $g(x)$, it follows that if $h(x) \mid f(x), g(x)$, then $h(x) \mid d(x)$. □

Example 2.37. Find $\gcd(2x^4 + x^3 - 6x^2 + 7x - 2, 2x^3 - 7x^2 + 8x - 4)$ over $\mathbb{Q}$.

Dividing the higher degree by the lower, we find that the quotient is $x + 4$ and remainder $14x^2 - 21x + 14 \implies 2x^2 - 3x + 2$.

$$\gcd(2x^3 - 6x^2 + 8x - 4, 2x^2 - 3x + 2).$$

Dividing again gives quotient $x - 2$ and no remainder, so the gcd is $x^2 - \frac{3}{2}x + 1$ (divided so monic).

Proposition 2.38

$p, f, g \in F[x]$. If $\gcd(p, f) = 1$, and $p \mid fg$, then $p \mid g$.

Definition 2.39. A nonconstant polynomial is **irreducible over the field** F if it cannot be factored in $F[x]$ into a product of polynomials of lower degree. **reducible** over F is one exists.

Proposition 2.40

A polynomial of degree 2 or 3 is irreducible over $F \iff$ it has not roots in F.

Lemma 2.41

The nonconstant polynomial $p \in F[x]$ is irreducible over $F \iff \forall f, g \in F[x]$, $p(x) \mid (f(x)g(x)) \implies p(x) \mid f(x)$ or $p(x) \mid g(x)$.

Theorem 2.42 (Unique Factorization)

Any nonconstant polynomial with coefficients in the field F can be expressed as some element in F times irreducible monic polynomials.

Proposition 2.43

A nonconstant polynomial $f(x)$ over $\mathbb{R}$ has no repeated factors $\iff$ $\gcd(f(x), f'(x)) = 1$.

Proof. Change to showing f only has repeated factor over $\mathbb{R} \iff \gcd(f(x), f'(x)) \neq 1$. So $\gcd(f(x), f'(x)) = d(x)$. Then $f(x) = a(x)p(x)$ and $f'(x) = b(x)p(x)$ for some irreducible factor p of d. Note that

$$f'(x) = a'(x)p(x) + a(x)p'(x) = b(x)p(x) \implies p(x) \mid a(x)p'(x).$$

Thus $p(x) \mid a(x)$, since p is irreducible and $p \nmid p'$. Therefore $f(x) = c(x)p(x)^2$ for some $c(x) \in F[x]$, and so $f(x)$ has a repeated factor.

Conversely, $f(x) = g(x)^n q(x)$ with $n > 1$ means that

$$f'(x) = ng(x)^{n-1}g'(x)q(x) + g(x)^n q'(x).$$

So g is a common divisor of f and f'. □

§2.7 Existence of Roots

Definition 2.44. If E, F are fields and $F \subseteq E$, then F is a **subfield** of E and E a **extension field** of F.

Definition 2.45. The set of all congruence classes modulo $p(x)$ will be denoted $F[x]/\langle p(x)\rangle$.

Proposition 2.46

Let F be a field, let $a(x), p(x) \in F[x]$ with $p(x)$ nonzero. If $p(x)$ is not a factor of $a(x)$, then the congruence class $[a(x)]$ modulo $p(x)$ contains exactly one polynomial $r(x)$ with $\deg(r(x)) < \deg(p(x))$.

Proposition 2.47

$a[x]$ in te last proposition has a multiplicative inverse in $F[x]/\langle p(x)\rangle \iff \gcd(a(x), p(x)) = 1$.

Theorem 2.48

For a field F and nonconstant polynomial p, then $F[x]/\langle p(x)\rangle$ is a field $\iff p(x)$ is irreducible over F.

Proof. We want to prove that $F/\langle p(x)\rangle$ has multiplicative inverses if and only if $p(x)$ irreducible, since the rest of the requirements for fields are easy to show. Each nonzero congruence class $[a(x)]$ has a multiplicative inverse if and only if $\gcd(a(x), p(x)) = 1$ for all nonzero polynomials $a(x)$ with $\deg(a(x)) < \deg(p(x))$. This occurs if and only if $p(x)$ is irreducible. □

Example 2.49 (Construction of Complex Numbers)**.** Since $x^2 + 1$ is irreducible in $\mathbb{R}$, we have $\mathbb{R}[x]/\left\langle x^2 + 1\right\rangle$ being a field. Each of the elements is bijective to some $a + bx$. So then the mapping

$$\phi : \mathbb{R}[x]/\left\langle x^2 + 1\right\rangle \to \mathbb{C}$$

defined as

$$\phi([a + bx]) = a + bi$$

is an isomorphism. Since $x^2 \equiv -1 \pmod{x^2 + 1}$, this is constructs the complex plane.

Theorem 2.50 (Kronecker)

Let F be field, and $f(x)$ any nonconstant polynomial in $F[x]$. $\exists$ an extension field E of F and an element $u \in E$ such that $f(u) = 0$.

Proof. $f(x)$ is a product or irreducible polynomials. Since $F[x]/\langle p(x)\rangle$ is field, we can denote it E. F is isomorphic to a subfield of E consisting of all congruence classes $[a]$ with $a \in F$. Let u be the congruence class $[x]$.

$$p(u) = a_n([x])^n + \cdots + a_1([x]) + a_0 = [a_n x^n + \cdots + a_1 x + a_0] = [0],$$

since $p(x) \equiv 0 \pmod{p(x)}$. □

Corollary 2.51

If $f(x) \in F[x]$, then there exists an extension field E over which $f(x)$ can be factored into a product of linear factors.

Example 2.52. For the polynomial $x^4 - x^2 - 2$, we have the factors $(x^2-2)(x^2+1)$ in $\mathbb{Q}$. Firstly, let $E_1 = \mathbb{Q}[x]/\langle x^2 - 2\rangle$, isomorphic to $\mathbb{Q}(\sqrt{2})$. Then let $E_2 = E_1/\langle x^2+1\rangle$. This field is $\mathbb{Q}(\sqrt{2}, i)$.

§2.8 Polynomials over $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$

For any root c of a polynomial $f(x)$, we must have $(c-n) \mid f(n)$. This fact can be used to find rational roots faster; if a value does not satisfy this, we can toss it out.

Definition 2.53. A polynomial with integer coefficients is called **primitive** if 1 and -1 are the only common divisors of its coefficients.

The gcd of the coefficients of a polynomial $p(x)$ is called the **content** of $p(x)$. Reminder that the **index** of a coefficient a_i in a polynomial is the i.

Lemma 2.54

Let p be a prime number, and $f(x) = g(x)h(x)$, where $f(x) = a_m x^m + \cdots + a_1 x + a_0$, $g(x) = b_n x^n + \cdots + b_1 x + b_0$, and $h(x) = c_k x^k + \cdots + c_1 x + c_0$. If b_s, c_t are the coefficients of least index not divisible by p, then a_{s+t} is the coefficient of least index not divisible by p.

Proof.

$$a_{s+t} = b_0 c_{s+t} + \cdots + b_{s-1}c_{t+1} + \boxed{b_s c_t} + b_{s+1}c_{t-1} + \cdots + b_{s+t}c_0.$$

All terms $b_0, \ldots, b_{s-1}$ and $c_{t-1}, \ldots, c_0$ are divisible by p by assumption.

Any term smaller $p \mid a_k = \sum_{i=0}^{k} b_i c_{k-i}$ □

Theorem 2.55 (Gauss' Lemma)

Product of two primitive polynomials is primitive.

Proof. Use the last lemma; since for any p, we can find a coefficient of $f(x) = g(x)h(x)$ that does not divide it, we conclude $f(x)$ is primitive. □

Theorem 2.56 (Eisenstein's Irreducibility Criterion)

$$f(x) = a_n x^n + \cdots a_1 x + a_0,$$

be a polynomial with integer coefficients. If there exists a prime number p such that

$$a_{n-1} \equiv a_{n-2} \equiv \cdots \equiv a_0 \equiv 0 \pmod{p},$$

but $a_n \not\equiv 0 \pmod{p}$ and $a_0 \not\equiv 0 \pmod{p^2}$, then $f(x)$ is irreducible over $\mathbb{Q}$.

To show that $p(x)$ is irreducible, it suffices to show that $p(x+c)$ is irreducible for some integer c. You cannot apply Eisenstein's Criterion to x^2+1, but you can if you replace x with $x+1$.

Corollary 2.57

If p prime, then

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$$

is irreducible over $\mathbb{Q}$.

Proof. Note that

$$\Phi_p(x) = \frac{x^p - 1}{x - 1},$$

so

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + \binom{p}{1} x^{p-2} + \cdots + p.$$

So all $a_{n-1} \ldots a_0$ are divisible by p, but a_n is not, and a_0 is not divisible by p^2, thus meeting Eisenstein's criterion. □

Therefore p being prime gives us

$$x^p - 1 = (x-1)(x^{p-1} + \cdots + 1),$$

but not necessarily for composite numbers:

$$x^4 - 1 = (x-1)(x+1)(x^2+1).$$

Definition 2.58. A complex nth root of unity is said to be **primitive** is it is a root of a polynomial $x^n - 1$ but not a root of $x^m - 1$ for any positive integer $m < n$.

Proposition 2.59

If $f(x) \in \mathbb{R}[x]$, then any complex root z must have its conjugate $\overline{z}$ as a root.

Theorem 2.60

Any polynomial of positive degree in $\mathbb{R}[x]$ can be factored into a product of linear and quadratic terms with real coefficients.

Proof. Factor out roots in $\mathbb{R}$. For each complex one, it has a conjugate, so make that quadratic $((x-z)(x-\overline{z}))$. □

In $\mathbb{R}[x]$, irreducible polynomials must be either

1. $ax + b$ with $a \neq 0$, or
2. $ax^2 + bx + c$ with $a \neq 0$ and $b^2 - 4ac < 0$.

§2.9 Chapter 4 End Remarks

If only positive coefficients and positive values of x were solutions to a cubic, solutions to these equations would suffice:

$$x^3 + px = q \tag{2.1}$$
$$x^3 = px + q \tag{2.2}$$
$$x^3 + q = px \tag{2.3}$$

The first was solved in 1526 by Scipione del Ferro. The second and third were solved by Cardano. but he swore to not reveal it. Lodovico Ferrari extended it to a general fourth degree equation. He published his solution with Ferrari in *Ars Magna* (1545), and got in a dispute with Tartaglia, the person he swore an oath with.

§3 Semester 3

§3.1 CHAPTER 5: Commutative Rings

Many group ideas can be extended to rings. There exist factor groups in rings: *factor rings*. Normal subgroups are like ideals. Ending part is on constructing quotient fields for integral domains, characterizing all subrings of fields.

§3.2 Commutative Rings; Integral Domains

Example 3.1. Key Rings to Know: $\mathbb{Z}, \mathbb{Z}_n$, any field F (i.e. $\mathbb{Q}, \mathbb{R}$), $F[x]$.

There is an **underlying additive group** for any ring R, just by the fact that the ring exists.

Definition 3.2. R is a **commutative ring** if it is **closed, associative, commutative, distributive, additive and multiplicative identity, additive inverse**.

$1 \neq 0$ is not required in a ring, therefore $\{0\}$ is a ring (the **zero ring**). If you prove multiplication is commutative, then you only need to show one of the distributive properties. The cancellation law may fail for multiplication: $2 \cdot 3 = 4 \cdot 3 \nRightarrow 2 = 4$ in $\mathbb{Z}_6$.

Definition 3.3. $R \subseteq S$ is a **subring** of S if it is commutative under addition and multiplication of S, and has the same identity as S.

Alternatively, you can show that (if R is commutative, $a \in R \implies -a \in R$, and R contains identity of S) $\iff$ R is a subring of S.

Example 3.4 (Check that Identity Matches!). Let $S = \{0, 2, 4\}$. $S \subseteq \mathbb{Z}_6$ It can be confirmed that S is a commutative ring, but since the identity is 4, it cannot be a subring.

Definition 3.5. $a \in R$ is **invertible** if $\exists b \in R$ such that $ab = 1$.
a is also called a **unit** of R and b is the multiplicative inverse of a (a^{-1}).
An element a such that $ab = 0$ for some $b \neq 0$ is called a **divisor of zero**.

Proposition 3.6

For any ring R, the set of all units, $R^\times$ is an abelian group under multiplication.

The multiplication cancellation law holds if and only if R has no nonzero divisors of zero.

Definition 3.7. A commutative ring R is called an **integral domain** if $1 \neq 0$ and $\forall a, b \in R$, $ab = 0 \implies a = 0$ or $b = 0$.

Example 3.8. If D is an integral domain, then $D[x]$ is also one. To show this, consider the leading coefficients.

Theorem 3.9

Any subring of a field is an integral domain.

Proof. Let R be a subring of F. It immediately inherits $1 \neq 0$. $ab = 0$ in R also holds in F. If $a = 0$, we're done. When $a \neq 0$, $ab = 0$ in F can be multiplied by inverse a on both sides, yielding $b = 0$. □

$\mathbb{Z}_n$ is an integral domain $\iff$ n prime, since $n \mid ab \implies n \mid a$ or $n \mid b$, n clearly must be prime. Why are integral domains and fields the same for $\mathbb{Z}_n$? Well...

Theorem 3.10

Any finite integral domain must be a field.

Proof. Let D be a finite integral domain, and D^* be the set without zero. If $d \in D$ and $d \neq 0$, then multiplication by d defines a function $f : D^* \to D^*$, $f(x) = xd$. f is clearly injective, but since it maps from a finite set to itself, it also must be surjective. So $1 = f(a)$ for some $a \in D^*$, so $ad = 1$ for some $a \in D$, and so each nonzero element of D is invertible. □

§3.3 Ring Homomorphisms

Definition 3.11. A function $\phi : R \to S$ is a **ring homomorphism** if:

1. $\phi(a + b) = \phi(a) + \phi(b)$,

2. $\phi(ab) = \phi(a)\phi(b)$,
3. $\phi(1) = 1$.

A **ring isomorphism** is when ϕ is also bijective. A **ring automorphism** happens if ϕ maps R to itself.

Proposition 3.12

If ϕ, θ are ring isomorphisms: ϕ^{-1} is a ring isomorphism, $\theta \circ \phi$ is a ring isomorphism.

a is a unit of $R \iff \phi(a)$ is a unit of S, moreover, R is a field $\iff S$ is a field.

Example 3.13 (Ring Homomorphism Examples)**.** Some examples:

1. The **natural projection**, $\pi : \mathbb{Z} \to \mathbb{Z}_n$, defined as $\pi(x) = [x]_n$.
2. The **natural inclusion**, $\iota : R \to R[x]$, defined as $\iota(a) = a$.
3. $\phi : \mathbb{Q}[x] \to R$ by $\phi(f(x)) = f(\sqrt{2})$. The image is $\mathbb{Q}(\sqrt{2})$.
4. **Evaluation mapping**. Let F be a subfield of E. For any element $u \in E$, let $\phi : F[x] \to E$ be defined by $\phi(f(x)) = f(u)$.

Proposition 3.14

If $\phi : R \to S$ is a ring homomorphism, then $\phi(0) = 0$, $\phi(-a) = -\phi(a) \forall a \in R$, and $\phi(R)$ is a subring of S.

Proposition 3.15

If $\phi : R \to S$ is a ring homomorphism, then

1. If $a, b \in \ker(\phi)$, and $r \in R$, then $a \pm b, ra \in \ker(\phi)$.
2. ϕ is an isomorphism $\iff \ker(\phi) = \{0\}$ and $\phi(R) = S$.

Theorem 3.16 (The Fundamental Theorem of Ring Homomorphisms)

If $\phi : R \to S$ is a ring homomorphism, then $R/\ker(\phi) \cong \phi(R)$.

Sketch. $\theta : R/\ker(\phi) \to \phi(R)$ defined as $\theta(a + \ker(\phi)) = \phi(a)$ works. □

Proposition 3.17

Let $\theta : R \to S$ be a ring homomorphism. For $s \in S, \exists$ a unique homomorphism $\widehat{\theta_s} : R[s] \to S$ such that $\widehat{\theta_s}(r) = \theta(r) \forall r \in R$, and $\widehat{\theta_s} = s$.

This should be thought of as an evaluation mapping; if $f(s) = 0$, then s is a **root**.

Definition 3.18. The set of n tuples of rings $R_1, \ldots, R_n$ is called the **direct sum** and is denoted:

$$R_1 \oplus R_2 \oplus \cdots \oplus R_n.$$

A useful takeaway is that if $n = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$, then we have

$$\mathbb{Z}_n \cong \bigoplus_{i=1}^{n} \mathbb{Z}_{p_i^{a_i}},$$

but we also have

$$\mathbb{Z}_n^{\times} \cong \bigoplus_{i=1}^{n} \mathbb{Z}_{p_i^{a_i}}^{\times},$$

which I am still a little confused on.

Definition 3.19. The smallest positive integer n such that $n \cdot 1 = 0$ (in R) is called the **characteristic** of R, denoted $\operatorname{char}(R)$. If no such integer exists, then R is said to have a **characteristic zero**.

We can think of $\operatorname{char}(R)$ as the exponent of the underlying additive group. Moreover, we can consider the homomorphism $\phi : \mathbb{Z} \to R$ defined by $\phi(n) = n \cdot 1$. The generator of $\ker(\phi)$ is the characteristic.

Proposition 3.20

An integral domain has characteristic 0 or p, a prime.

Proof. Consider ϕ as defined before for an integral domain D. The fundamental theorem for ring homomorphisms shows that $\mathbb{Z}/\ker(\phi)$ is isomorphic to the subring $\phi(\mathbb{Z})$ of D. But $\phi(\mathbb{Z})$ also has the property that it has no nontrivial divisors of zero, and therefore must be an integral domain. Either $\ker(\phi) = 0 \implies \operatorname{char}(D) = 0$, or $\ker(\phi) = n\mathbb{Z}$. This means that n must be prime, so $\operatorname{char}(D)$ is also prime. □

§3.4 Ideals and Factor Rings

Definition 3.21. An **ideal** is a subset I of R such that

- $a \pm b \in I \forall a, b \in I$,
- $ra \in I \forall a \in I, r \in R$.

If $1 \in I$, then it must be the whole ring R!

Proposition 3.22

Let R be a commutative ring with $1 \neq 0$. Then R is a field $\iff$ it has no proper nontrivial ideals.

Definition 3.23. Let R be a commutative ring, and $a \in R$. The ideal Ra is called a **principal ideal** generated by a.

An integral domain where every ideal is principally generated is called a **principal ideal domain**.

Example 3.24 (Polynomials Over a Field is a PID)**.** If I is any nonzero ideal of $F[x]$, then $f(x)$ is a generator for $I \iff$ it has a minimal degree among the nonzero elements of I. Since the generator of I is a divisor of every element of I, there is only one monic generator for I.

Definition 3.25. Let I be an ideal of a ring R. The ring R/I is called a **factor ring** of R modulo I.

Proposition 3.26

Let I be an ideal of R.

1. The natural projection $\pi : R \to R/I$ defined as $\pi(a) = a + I \forall a \in R$ is a ring homomorphism and $\ker(\pi) = I$.
2. There is a bijection between ideals of R/I and ideals of R that contain I.

   That bijection is: For each ideal J of R/I, we assign the ideal $\pi^{-1}(J)$ of R; to each ideal J of R, we assign the ideal $\pi(J)$ of R/I.

Sketch. Addition parts follow from a previous proof. The multiplication follows from definition of congruence classes.

If J is an ideal of R that contains I, then it corresponds to the additive subgroup

$$\pi(J) = \{a + I \mid a \in J\}.$$

Group things follow. On the other hand, if J is an ideal of R/I, then it corresponds to the subgroup

$$\pi^{-1}(J) = \{a \in R \mid a + I \in J\}.$$

□

Example 3.27. Let $R = \mathbb{Q}[x, y]$, and let $I = \langle y \rangle$. In forming R/I, we make the elements of I congruent to 0. We can find a definition as $\phi(f(x, y)) = f(x, 0)$. It is clear that $\ker(\phi) = \langle y \rangle$. $\mathbb{Q}[x, y]/\langle y \rangle \cong \mathbb{Q}[x]$ by fundamental theorem of homomorphisms of rings.

Definition 3.28. An proper ideal I of a commutative ring R is a **prime ideal** if for all $a, b \in R$ it is true that $ab \in I \implies a \in I$ or $b \in I$.

I is said to be a **maximal ideal** of R if for all ideals J of R, such that $I \subseteq J \subseteq R$, either $J = I$ or $J = R$.

We can see that if R is a ring with $1 \neq 0$, then R is an integral domain $\iff$ the the trivial ideal is the only prime ideal. In $\mathbb{Z}$, the trivial ideal is prime but not maximal.

Example 3.29. Let $\phi : R \to S$ be a ring isomorphism. Let I be any ideal of R. Let π be the natural projection from S onto $S/\phi(I)$. Consider $\overline{\phi} = \pi\phi$. Then $\overline{\phi}$ is surjective since both π and ϕ are, and

$$\ker(\overline{\phi}) = \{r \in R \mid \phi(r) \in \phi(I)\} = I.$$

Therefore $R/I \cong S/\phi(I)$.

Proposition 3.30

Let I be a proper ideal of the commutative ring R.

1. R/I is a field $\iff$ I is a maximal ideal of R
2. R/I is an integral domain $\iff$ I is a prime ideal of R
3. If I is a maximal ideal, then it is a prime ideal.

Proof. (1) Since I is a proper ideal of R, it does not contain 1. Therefore $1 + I \neq 0 + I$.

$$\begin{aligned} R/I \text{ is a field} &\iff \text{it has no proper nontrivial ideals} \\ &\iff \text{there are no ideals properly between } I \text{ and } R \\ &\iff I \text{ is maximal.} \end{aligned}$$

(2) ($\implies$) Let $a, b \in R$ with $ab \in I$. Assume R/I is an integral domain. For cosets of R/I, we have $(a + I)(b + I) = ab + I = 0 + I$. By assumption, this means either $a + I$ or $b + I$ is the zero coset. So either $a \in I$ or $b \in I$, so I is a prime ideal.

($\impliedby$) Assume that I is a prime ideal. Then $a, b \in R$, such that $(a+I)(b+I) = 0 + I$ in $R/I \implies ab \in I$. So by assumption $a \in I$ or $b \in I$. So $a + I$ or $b + I$ is the zero coset, making R/I an integral domain.

(3) follows from the other two. □

Ring isomorphisms preserve prime/maximal ideals.

Theorem 3.31

Every nonzero prime ideal of a principal ideal domain is maximal.

Proof. Let P be a nonzero prime ideal of PID R, and J be any ideal with $P \subseteq J \subseteq R$. We can assume $P = Ra$ and $J = Rb$ since R is a PID. $a \in P \implies a \in J$, so $a = rb$ for some $r \in R$. So $rb \in P$; either $b \in P$ or $r \in P$, since P is prime. If $b \in P$, then it can be principally generated by b, so $P = J$. Otherwise, $r \in P \implies r = sa$ for some $s \in R$. So $a = sab$. Since R is an integral domain, this reduces to $1 = sb$. Shows that $1 \in J \implies J = R$. ☐

Example 3.32 (Ideals of Polynomials). Let F be any field. The nonzero ideals of $F[x]$ are all principal, of the form $\langle f(x) \rangle$, where $f(x)$ is any polynomial of minimal degree in the ideal. The ideal is prime (and hence maximal) $\iff f(x)$ irreducible. Therefore if $p(x)$ is irreducible, then $F[x]/\langle p(x) \rangle$ is a field.

Example 3.33 (Kernel and Image of the Evaluation Mapping). Let F be a subfield of E. Let the evaluation mapping be defined for $u \in E$ as:

$$\phi_u : F[x] \to E \qquad \phi_u(f(x)) = f(u).$$

ϕ_u defines a ring homomorphism.

Also, $\phi_u(F[x])$ is a subring of E, and therefore an integral domain.

This image is isomorphic to $F[x]/\ker(\phi_u)$, so $\ker(\phi_u)$ is a prime ideal.

As long as this is nonzero, it is a maximal ideal as well.

Therefore we conclude that $F[x]/\ker(\phi_u)$ is a field, so the image of ϕ_u is a subfield of E.

§3.5 Quotient Fields

The goal is to show that any integral domain is isomorphic to a subring of a field. The next step is constructing "fractions" with numerator and denominator in an integral domain D.

Lemma 3.34

Let D be an integral domain, and

$$W = \{(a, b) \mid a, b \in D \text{ and } b \neq 0\}.$$

The relation $\sim$ for W defined by $(a, b) \sim (c, d)$ if $ad = bc$ is an equivalence relation.

We will denote each class (a, b) by $[a, b]$, and the set of all classes by $Q(D)$.

Lemma 3.35

The operations for $Q(D)$ are

$$[a, b] + [c, d] = [ad + bc, bd] \qquad [a, b] \cdot [c, d] = [ac, bd],$$

and are well-defined.

Theorem 3.36

Let D be an integral domain. Then $Q(D)$ is a field that contains a subring isomorphic to D.

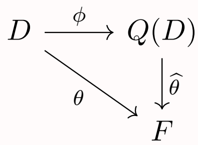
Proof. We first need to show that $Q(D)$ is a field, which is easy to see.

Consider the mapping $\phi : D \to Q(D)$ defined by $\phi(d) = [d, 1] \forall d \in D$. ϕ clearly preserves sums and products. $\phi(1) = [1, 1]$, the identi ty of $Q(D)$, so ϕ is a ring homomorphism. $\ker(\phi)$ can only be $\{0\}$. Therefore $\phi(D)$ is a subring of $Q(D)$ that is isomorphic to D. □

Definition 3.37. $Q(D)$ is called the **field of quotients/fractions** of an integral domain D.

Theorem 3.38

For ϕ as defined in the last theorem, if there is a function $\theta : D \to F$ that is injective to a field F, then there exists a unique ring homomorphism $\widehat{\theta} : Q(D) \to F$ that is injective, such that $\widehat{\theta}\phi(d) = \theta(d) \forall d \in D$.



Proof. For $[a, b] \in Q(D)$, let $\widehat{\theta}([a, b]) = \theta(a)\theta(b)^{-1}$. Need to show that it is well defined, and unique. □

Change in notation: using a/b instead of $[a, b]$ for the equivalence classes of $Q(D)$.

Corollary 3.39

Let D be an integral domain that is a subring of a field F. If each element has the form a/b for $a, b \in D$, then $F \cong Q(D)$.

Example 3.40. Let D be the integral domain of all fractions $a/b \in \mathbb{Q}$ such that n is odd. If for a/b, $\gcd(a, b) = 1$, then either they are both odd, meaning $a/b \in D$, or b is even, meaning that $(a/b)^{-1} = b/a \in D$. Therefore $\mathbb{Q} \cong Q(D)$.

Corollary 3.41

Any field contains a subfield isomorphic to $\mathbb{Q}$ or $\mathbb{Z}_p$.

Proof. Let F be any field, and let $\phi : \mathbb{Z} \to F$ be defined by $\phi(n) = n \cdot 1$. If $\ker(\phi) \neq \{0\}$, then it is $p\mathbb{Z}$ for some prime p. So the image is a subfield isomorphic to $\mathbb{Z}_p$.

If ϕ is injective, then the last theorem tells us there is a homomorphism from $Q(\mathbb{Z})$, or $\mathbb{Q}$ into F. The image is a subfield of F isomorphic to $\mathbb{Q}$ in this case. □

§3.6 Chapter 5 End Remarks

Terminology for these structures came from a paper in 1897 by David Hilbert(1862-1943). He recognized that ideal theory was closely related to algebraic geometry. Many abstract algebra discoveries were made by Emmy Noether (1882-1935).