Group Theory

Zac Zerafa

July 19, 2026

Contents

Part I

Fundamentals

Mathematical logic Set theory Group theory

Chapter 1

Rings

Groups are powerful algebraic structures, but they only consider one operation. We don't yet have the language to talk about how two operations interact with eachother. A few notions that we're familiar with from elementary algebra and elementary number theory are not adequately generalized by group theory alone.

Ring theory develops the necessary theory to model algebraic structures with two operations, however it still draws heavily on group theory.

1.1 Rings

Definition 1.1 (Ring)**.** A *ring* is a 3-tuple $(R, +, \times)$ of a set R and operations $+, \times$ such that:

- $(R, +)$ is an Abelian group
- $(R, \times)$ is a monoid
- $x \times (y + z) = x \times y + x \times z$ ($\times$ is left distributive with respect to $+$)
- $(y + z) \times x = y \times x + z \times x$ ($\times$ is rightdistributive with respect to $+$)

We write 0_R as the identity element of $(R, +)$ and 1_R the identity element of $(R, \times)$. We often write $r \times s$ as rs, and call $\times$ by the name R-multiplication and $+$ as R-addition. When the operations are apparent, a ring $(R, +, \times)$ may be denoted as R.

When the operations are apparent, a ring $(R, +, \times)$ may be denoted as R, and the multiplication expression $r \times s$ may be contracted to rs. Note that when speaking generally about rings, 'addition' refers to the ring operation forming the Abelian group and 'multiplication' refers to the ring operator forming the monoid.

With multiplication of arithmetic, sometimes $\cdot$ is used as another symbol for multiplication; we avoid this use because we reserve that symbol for a different operation called 'scalar multiplication' which will shpw up in module theory.

We will denote inverse elements with repect to addition by a minus sign rather than our familiar '-1 exponent' (it'll be clear soon why), so the additive inverse of r is denoted as $-r$.

1.2 Properties of rings

It is useful to understand the fundamental properties of rings before proceeding further with ring theory.

Proposition 1.1. Let $(G, \times)$ be a group:

- 0_R is an absorbing element; multiplication with 0_R is always 0_R

$$\forall r \in R$$
$$r0_R = 0_R r = 0_R$$
$$(-1_R)r = r(-1_R) = -r$$
$$-(rs) = r(-s) = (-r)s$$

Proposition 1.2.

Proposition 1.3. If $1_R = 0_R$, then R is the trivial ring; the only element in the ring is 0_R.

$$1_R = 0_R \implies (R, +, \times) \cong (\{0\}, +, \times)$$

Many concepts from group theory translate easily to ring theory.

Definition 1.2 (Order of a ring)**.** The *order* of a ring is the cardinality of its set.

Definition 1.3 (Finite ring)**.** A *finite ring* is a ring with finite order.

Definition 1.4 (Commutative ring)**.** A *commutative ring* is a ring such that multiplication is commutative.

Definition 1.5 (Subring)**.** A *subring* of $(R, +, \times)$ is a ring $(S, +, \times)$ such that $(S, +)$ is a subgroup of $(R, +)$ and $(S, \times)$ is a subgroup of $(R, \times)$.

That said, there are some unique concepts in ring theory that describe the relationship between its Abelian group and monoid.

1.3 Zero divisors and units

Definition 1.6 (Zero divisor)**.** An element $x \in R \setminus \{0\}$ of a ring is a *zero divisor* iff there is a $y \in R \setminus \{0\}$ such that $xy = yx = 0$.

Multiplication in rings is a monoid rather than a group, so there is no guarantee of inverse elements. However, it is possible that some elements are invertible with respect to multiplication; such elements are called *units*.

Definition 1.7 (Unit)**.** An element $x \in R$ of a ring is a *unit* iff there is a $y \in R$ $xy = yx = 1_R$. For a group R, denote its set of units as R^*.

Like groups, inverse elements are unique (when they exist). We will denote the multiplicative inverse of the unit r as r^{-1}.

Proposition 1.4. If r is a unit of R, there exists a unique r^{-1} such that $rr^{-1} = r^{-1}r = 1_R$

Proposition 1.5. If r is a unit of R, then r^{-1} is a unit of R.

1.4 Domains

Definition 1.8 (Domain)**.** A *domain* D is a ring with no zero divisors.

$$D \text{ is a domain} \iff D \text{ is a ring } \wedge \{d \in D \setminus \{0_D\} : \exists e[de = ed = 0_D]\} = \emptyset$$

Proposition 1.6 (Cancellation law for domains)**.** Let $(D, +, \times)$ be a domain, if $a \neq 0_R$ and $ax = ay$ then $x = y$.

1.5 Fields

Definition 1.9 (Field)**.** A *field* F is a commutative ring with where all elements except for 0_F are units.

$$(F, +, \times) \text{ is a field } \iff (F, +, \times) \text{ is a commutative ring } \wedge F^* = F \setminus \{0_F\}$$

If the whole ring (save the additive identity) are units, then all elements are invertible and hence R-multiplication upgrades from a monoid to a group. Futhermore, if the ring is commutative then it becomes an Abelian group.

This insight gives an alternative perspective to view fields from.

Proposition 1.7 (Alternate definition of a field)**.** A ring $(F, +, \times)$ is a field iff $(F, \times)$ is an Abelian group.

$$(F, +, \times) \text{ is a field } \iff (F, +, \times) \text{ is a ring } \wedge (F, \times) \text{ is an Abelian group}$$

The fact that all elements are units in fields eradicates the possibility of zero divisors; consider the following equation where $r \neq 0$.

$$rs = 0$$

Since $r \neq 0$ it is invertible, hence we can do the following.

$$r^{-1}rs = r^{-1}0$$

$$r^{-1}rs = 0$$

$$s = 0$$

Because of this property of fields we can never have zero divisors; fields are a special type of domain.

Proposition 1.8. Fields are domains.

$$F \text{ is a field } \implies F \text{ is a domain}$$

1.5.1 Field extension

E is a field extension of F iff F is a subfield of E S is a field extension of R iff R is a subring of S

1.5.2 Algebraic extension

Special type of field extension $\mathbb{R}(i)$ $\mathbb{Q}(\sqrt{2})$

Chapter 2

Quotient rings

2.1 Ideals

Consider a subgroup N. In group theory we based quotient groups on the following equivalence relation.

$$g \sim h \iff h^{-1}g \in N$$

For the quotient map to be well defined however, requiring N to be a normal subgroup is necessary and sufficient.

In ring theory, we take left cosets with respect to subgroups of the additive group, so we have the following.

$$r \sim s \iff r - s \in I$$

By the definition of a ring, I is Abelian and therefore normal, however we require an extra condition for the quotient map to be well defined with multipliction.

$$(r + i)(s + j) = rs + rj + si + ij$$

We want some expression $rs+i_*$, by assuming that $ri \in I$ for any ring element r and any $i \in I$, then $rj + si + ij \in I$ and hence $rs + (rj + si + ij) \in rs + I$

Such an I is called an *right-sided ideal*.

Remember quotient groups? It's quite nice that cosets partition a group (thanks Lagrange); this along with the ability of normal subgroups to make our quotient map a well defined group homomorphism allowed the creation of a group on these 'divided' equivalence classes. In group theory, quotient

groups must be formed from normal subgroups to ensure that the quotient group operation functions as desired. One may ask; what's the ideal (pun intended) subring that can be used to make a notion of a 'quotient ring'?

Unfortunately, subrings won't do the the trick, but if we want to emulate the idea of left multiplication cosets, we can form some kind of set that would ideally (this joke is going to get seriously overused in this part) do the trick.

Definition 2.1 (Two sided ideal)**.** Let $(R, +, \cdot)$ be a ring. A *two-sided ideal of* R is a subgroup I of $(R, +)$ closed under multiplication from any element in R. For brevity, two-sided ideals will just be called ideals.

$$(I, +) \leq (R, +) \wedge \forall r \in R \forall i \in I [ri \in I \wedge ir \in I]$$

Proposition 2.1 (Alternative definition for an ideal)**.** Let $(R, +, \cdot)$ be a ring. A *two-sided ideal of* R is a subgroup I of $(R, +)$ closed under addition, multiplication, and multiplication from any element in R. For brevity, two-sided ideals will just be called ideals.

$$r \in R, i, j \in I$$

$$i + j \in I$$

$$ij \in I$$

$$ri \in I$$

$$ir \in I$$

One can define specific ideals where arbitrary ring multiplication is allowed only from the left or right.

Definition 2.2 (Left ideal)**.** Let $(R, +, \cdot)$ be a ring. A *left ideal of* R is a subgroup I of $(R, +)$ closed under addition, multiplication, and left multiplication from any element in R.

$$r \in R, i, j \in I$$

$$i + j \in I$$

$$ij \in I$$

$$ir \in I$$

We'll focus our attention on two-sided ideals from now on.

Proposition 2.2. If $1_R \in I$, then $I = R$.

Proposition 2.3. Let $I, J \subseteq R$ be ideals, then $I \cap J$ is an ideal of R.

We can also define the sum of ideals, which is an ideal itself.

Definition 2.3 (Sum of ideals)**.**

$$I + J = \{i + j : i \in I \wedge j \in J\}$$

2.2 Ideal generating notation

Consider R as a commutative ring, since $(R, +)$ is an Abelian group, any element $r \in R$ generates its own cyclic subgroup of $(R, +)$, to make this set a (double-sided) ideal we just need to close this with multiplication over any ring element.

$$\langle x \rangle = \{\lambda x : \lambda \in R\}$$

Why does this form an ideal? The elements of the cyclic subgroup of x are representable as $\sum_{i=1}^{n} x$. Since λ is an arbitrary ring element, we can consider lambdas of the form $\lambda = \sum_{i=1}^{n} 1_R$ so that we have $(\sum_{i=1}^{n} 1_R)x = \sum_{i=1}^{n} x$ which is in the cyclic subgroup. Since λ is again an arbitrary ring element, letting it be of the form $\lambda = r(\sum_{i=1}^{n} 1_R)$ where $r \in R$ satisfies all properties of an ideal.

Since

$$\langle x_1, x_2, \cdot x_n \rangle = \{\sum_{k=1}^{n} \lambda_k x_k : \lambda_k \in R\}$$

$$\langle X \rangle = \{\sum_{k=1}^{n} \lambda_k x_k : \lambda_k \in R \wedge x_k \in X\}$$

Note that when using this notation. We require topological structure to have a notion of convergence, therefore we can only consider finite sums when generating ideals (if you're familiar with linear algebra, perhaps one could compare X generating the ideal in a way similar to a Hamel basis).

$$\langle ij : i \in I, j \in J \rangle$$

$$\langle r_1 r_2, \ldots, r_n \rangle = \{\sum_{k=1}^{n} \lambda_k r_k : \lambda_k \in R\}$$

$$\langle f : f \in M \rangle = \{\sum_{f_k \in N} \lambda_k f_k : \lambda_k \in R, N \subseteq M, |N| < \infty\}$$

Ideals equal to some are 'finitely generated'.

With ideal generating notation, we can now produce a sleek definition for the product of ideals.

Definition 2.4 (Product of ideals)**.**

$$IJ = \langle \{ij : i \in I \wedge j \in J\} \rangle$$

2.3 Basic types of ideals

2.3.1 Zero ideals

Definition 2.5. Let $(R, +, \cdot)$ be a ring, then $\{0_R\}$ is the *zero ideal*.

We should check that this definition is well defined, that is, this set is indeed always an ideal. When describing the ideals over a certain ring, We'll often need to tag along the fact that the zero ideal is an ideal over said ring; otherwise there's not too much to say about it.

Proposition 2.4. Let I be a ideal of the field $(F, +, \cdot)$, then either I is the zero ideal or $I = F$.

2.3.2 Unit ideals

We've proven that when the identity is in our ideal, the ideal must be the whole ring. This is another trivial ring that we may as well mention for completeness.

Definition 2.6. Let $(R, +, \cdot)$ be a ring, then R is the *unit ideal*.

2.3.3 Principle ideal

Definition 2.7. A *principal ideal* is an ideal of the form $\langle d \rangle$. In other words, it is generated by one element.

If D is a domain where all its ideals are principal ideals, PID (principal ideal domain).

Example 2.1. $(\mathbb{Z}, +, \cdot)$ is a PID and all its ideals are $d\mathbb{Z}$. This is because the only subgroups of $(\mathbb{Z}, +)$ are of the form $d\mathbb{Z}$, and these can be verified to be principal ideals since addition is obviously satisfied (being a subgroup), multiplication in and out of the ideal is satisfied since $r(dn) = d(rn) \in d\mathbb{Z}$. Note that $0\mathbb{Z}$ corresponds to the zero ideal.

Example 2.2.

2.4 Quotient rings

Definition 2.8. A *quotient ring on R* is a ring of unique left 'addition' cosets on the ideal I. Addition and multiplication are defined in the following way.

$$(R/I, \oplus, \otimes)$$

$$(r + I) \oplus (s + I) = (r + s) + I$$

$$(r + I) \otimes (s + I) = rs + I$$

We should make sure that $\oplus, \otimes$ are well defined operations; we didn't introduce ideals for nothing!

For the sake of simplicity, we'll often use the equivalence class notation $[r] = r + I$ with the original ring's addition and multiplication symbols $+, \times$ for elements, addition, and multiplication of a quotient ring. Here's an example below.

$$(r + I) \otimes ((s + I) \oplus (t + I)) = [r]([s] + [t])$$

2.4.1 Examples of quotient rings

2.5 Prime ideal

For quotient groups, there aren't many general properties of the normal subgroup that give interesting properties to the quotient group. For quotient

rings, the properties of the ideal used in the quotient ring can say a great deal regarding the quotient ring's properties.

For instance, One may want to know when a quotient ring is a domain; this question happens to depend greatly on the nature of the ideal.

Recall that domains are categorized by the fact that $xy = 0_D$ iff either x, y equals 0_D. $[0_D]$ is the left coset representing the domain itself, so assuming our quotient ring is a domain, when $[x][y] = [0_R]$ (in other words, when $xy \in I$), either $[x]$ or $[y]$ equals $[0_R]$ (in other words, $x \in I$ or $y \in I$); meaning that one of them is in the same coset (the ideal) as 0_R.

This allows us to forge precisely the right ideal that makes a quotient ring a domain.

Definition 2.9. A *prime ideal* I is an ideal such that for any ring elements r, s, if rs is in the ideal, then either r or s is in the ideal.

Note that this looks slightly similar to Euclid's lemma! The difference being that it is inclusion of an ideal rather than divisibility by a prime.

Proposition 2.5. R/I is a domain iff I is a prime ideal.

2.6 Maximal ideal

Similarly, one wants to know which type of ideal forms a field. Assuming that the original ring is a commutative ring and we've made a quotient ring that is a field, we have

$[r][s] = [rs] = [1_R]$ so for any $r \notin I$, there is some $s \in R$ such that $rs - 1_R \in I$.

Now imagine a strictly larger ideal J such that $r \in J$. Since $rs \in J$ and $rs - 1_R \in J$, we can prove that $1_R \in J$ which means $J = R$. Since r was chosen arbitrarily, this means quotient rings that are fields have the largest non-unit ideal possible on the commutative ring.

Definition 2.10 (Maximal ideal)**.** A *maximal ideal* I is an ideal such that any ideal J where $I \subset J$ equals the entire ring.

Proposition 2.6. R/I is a field iff I is a maximal ideal.

since for a field R/I with an ideal J with $I \subset J$, we have both $rs - 1_R \in J$ and $rs \in J$ for some $r \in J, r \notin I$, and therefore$1_R \in J$, meaning that $R = J$.

Here's a proof sketch for the other direction: if I is maximal then for any $j \notin I$ we have $I \oplus \langle j \rangle = R$. Since $1_R \in R$, we have the expression $i + rz = 1_R$, where $i \in I, z \in \langle j \rangle, r \in R$, so then by the properties of ideals $rz \in \langle j \rangle$. We then have $rz - 1_R = -i$ so $rz - 1_R \in I$. Since r is an arbitrary ring element, this holds for any element in the commutative ring.

Since prime ideals and maximal ideals have a direct correspondence to domains and fields respectively, we can prove the following.

Corollary 2.1. Maximal ideals are prime ideals.

2.7 Generalized number theory in integral domains

Let's generalize number theory in an integral domain.

Definition 2.11 (Divisibility in an integral domain)**.**

$$a|r \iff \exists k \in R[ak = r]$$

Definition 2.12 (Reducible element)**.** r is irreducible iff it is not a unit nor 0 and the following holds.

$$r = ab \implies a \in R^* \vee b \in R^*$$

Definition 2.13 (GCD in an integral ring)**.**

$$\gcd(a, b) = n \iff \forall d \in R[d|a \wedge d|b \implies d|n]$$

A ring such that any pair of elements have a GCD is called a GCD domain

Proposition 2.7. PIDs are GCD domains.

Lemma 2.1 (Euclid's lemma (ring theory))**.** Let R be a GCD domain

$$n|ab \wedge \gcd(n, a) = 1_R \implies n|b$$

Lemma 2.2 (Bézout's lemma (ring theory))**.** Let R be a PID

$$\exists x, y \in R[ax + by = \gcd(a, b)]$$

Chapter 3

Ring homomorphisms

3.1 Ring homomorphism

Definition 3.1 (Ring homomorphism)**.** Let $(R, +_R, \cdot_R)$ and $(S, +_S, \cdot_S)$ be two rings. A *ring homomorphism* $f : R \to S$ is a function between rings that 'preserves' the ring's operation in the following sense; if r_1, r_2 are elements of R, we have the following.

$$f(r_1 +_R r_2) = f(r_1) +_S f(r_2)$$

$$f(r_1 \cdot_R r_2) = f(r_1) \cdot_S f(r_2)$$

$$f(1_R) = 1_S$$

Definition 3.2 (Alternative definition for a ring homomorphism)**.** Let $(R, +_R, \cdot_R)$ and $(S, +_S, \cdot_S)$ be two rings. A function $f : R \to S$ is a ring homomorphism iff f is a group homomorphism from $(R, +_R)$ to $(S, +_S)$ and the following 'monoid homomorphism' rule holds.

$$f(r_1 \cdot_R r_2) = f(r_1) \cdot_S f(r_2)$$

We may also want to consider a variant where we drop the requirement of $f(1_R) = 1_S$; rngs don't assume the existence of such an object, hence this condition doesn't make sense in that context. Even if it does exist, we may want to consider this weaker definition of a homomorphism in certain contexts anyway. Since this definition is the best that can be done for a rng, we call it a rng homomorphism.

Definition 3.3 (Rng homomorphism)**.** Let $(R, +_R, \cdot_R)$ and $(S, +_S, \cdot_S)$ be two rngs. A *rng homomorphism* $f : R \to S$ is a function between rings that 'preserves' the rng's operation in the following sense; if r_1, r_2 are elements of R, we have the following.

$$f(r_1 +_R r_2) = f(r_1) +_S f(r_2)$$

$$f(r_1 \cdot_R r_2) = f(r_1) \cdot_S f(r_2)$$

3.2 Properties of ring homomorphism

3.3 Examples of ring homomorphism

3.4 Ring monomorphism

3.5 Ring epimorphism

3.6 Ring endomorphism

These types of ring homorphisms have particularly interesting properties, but ring isomorphisms are perhaps the most important class of homomorphisms.

Chapter 4

Ring isomorphism

4.1 Properties of Ring isomorphism

4.2 Examples of Ring isomorphism

4.3 Ring automorphism

Some Theorems

A *Canonical map* is a function between two objects that arises from their definitions. It is a function used to define the behaviour of some object.

Definition 4.1 (Kernel (ring homomorphism))**.**

$$\ker(f) = \{r \in R : f(r) = 0_S\}$$

Definition 4.2.

$$\mathrm{Im}(f) = \{f(r) \in H : r \in R$$

Proposition 4.1.

$$f : R \to S \text{ is a ring homomorphism } \implies \mathrm{Im}(f) \leq S$$

Image

Isometry

4.4 First isomorphism theorem

The first isomorphism theorem generalizes to rings.

Lemma 4.1.

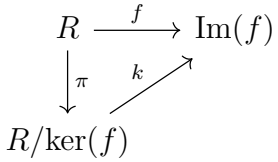
$$f : R \to S \text{ is a ring homomorphism } \implies \ker(f) \text{ is an ideal of } R$$

Lemma 4.2.

$$f : R \to S \text{ is a ring homomorphism } \implies [r_1{+}\ker(f) = r_2{+}\ker(f) \iff f(r_1) = f(r_2)]$$

Theorem 4.1 (First isomorphism theorem for rings)**.** Let $f : R \to S$ be a ring homomorphism . Then $\mathrm{Im}(f) \cong R/\ker(f)$ the following isomorphism k.

$$k : r + \ker(f) \mapsto f(r)$$



Proposition 4.2. For any ring R, the following $f : \mathbb{Z} \to R$ is a ring homomorphism.

$$f(n) = \sum_{i=1}^{n} 1_R$$

Though we've proven this ring version of the theorem by expressing our ideas with the objects of ring theory rathee than group theory, the machinery of category theory provides a natural way to extend certain "theorems" to a plethora of structures; such results are called universal properties in category theory.

Mathematical ranting aside, we can now prove some new results.

Ring homomorphisms between 2 fields are injective.

let $f : F \to K$ be a ring homomorphism For any subfield $F' \leq F$, $f(F')$ is a subfield of K For any subfield $K' \leq K$, $f^{-1}(K')$ is a subfield of F

Let S be a set of ring homomorphisms $F \to K$, then $Eq(S)$ is a subfield of F

4.5 Ring characteristic

Imagine we want to make ring homomorphisms from $\mathbb{Z}$, one can show that there is a unique homomorphism from $\mathbb{Z}$ to any ring.

$$f(n) = f(\sum_{k=1}^{n} 1) = \sum_{k=1}^{n} f(1) = \sum_{k=1}^{n} 1_R$$

We will now introduce the idea of a ring characteristic; a value that characterizes when this ring wraps back to 0_r, essentially determining the nature of how this homomorphism acts on a ring.

Definition 4.3 (Ring characteristic)**.** The *ring characteristic* is the order of the cyclic subgroup generated by the multiplicative identity.

$$\text{char}(R) = \text{ord}_+(1_R)$$

If the subgroup has infinite order, we say it has characteristic 0.

This homomorphism is special; it essentially means that $\mathbb{Z}$ lives inside every ring, integers being interpreted as n repeated additions of the multiplicative identity. This can go for groups too; take the cyclic subgroup generated by some element g and define the group homomorphism $f(n) = g^n$. By the first isomorphism theorem for groups, this is isomorphic to some $\mathbb{Z}/n\mathbb{Z}$; the concept is similar, though in rings this exists in a more canonical way.

Back to rings, let's see how this homomorphism interacts with 'modular' rings (rings with non-zero characteristic).

For rings with characteristic n, the kernel of f will be $n\mathbb{Z}$, so by the first isomorphism theorem for rings $f : \mathbb{Z}/n\mathbb{Z} \to R$ is a ring isomorphism on $f(\mathbb{Z}/n\mathbb{Z})$, but since the image of this function is merely a subgroup of R, it is a monomorphism on R.

Proposition 4.3. For any ring R, the following $f : \mathbb{Z}/\text{char}(R)\mathbb{Z} \to R$ is a ring monomorphism.

$$f(n) = \sum_{i=1}^{n} 1_R$$

Notice that if R is isomorphic to $\mathbb{Z}$ (repeated addition of multiplicative identity reaches all elements and never 'wraps' back to 0_R), the kernel is $0\mathbb{Z}$; this is why we use the conventionn of giving infinite order subgroups characteristic 0.

4.5.1 Theorems related to this special homomorphism

By noticing that some $\mathbb{Z}/n\mathbb{Z}$ lives in every ring, we can prove some interesting results.

Proposition 4.4. Let D be a domain, then $\text{char}(D)$ is either prime or 0.

If D is a finite domain, then the $f(\mathbb{Z}/\text{char}(R)\mathbb{Z})$ living inside must be a domain too since it is a subring. From our study in group theory however $\mathbb{Z}/n\mathbb{Z}$ with nonprime n permit zero divizors, hence $\text{char}(R)$ must be prime.

Theorem 4.2 (Freshman's dream)**.**

$$(x+y)^{p^r} = x^{p^r} + y^{p^r}$$

4.5.2 Frobenius map

$$f(r) = r^p$$

let p be prime, R be a commutarive ring of characteristic p then the Fobenius map is a homomorphism

If F is a finite of characteristic p then the frobenius map is an automorphism

Chapter 5

Field of fractions

The rationals are a big step up from the integers because it allows for multiplicative inverses (i.e it allows division). $\mathbb{Z}$ is only a domain, but $\mathbb{Q}$ forms a field.

Given any commutative domain, can we define a general way synthesize a field from it, analogous to transforming the domain $\mathbb{Z}$ to the field $\mathbb{Q}$? Of course one could just add synthetic units to form a field, however it is possible (and much more interesting) to create a system that is faithful to the algebra of fractions.

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

$$\text{frac}(R) = (R \times R \setminus \{\})/\sim$$

$$(a, s) + (b, t) = (at + bs, st)$$

$$(a, s)(b, t) = (ab, st)$$

We conventionally represent (a, s) as $\frac{a}{s}$

Just like how $\mathbb{Z}$ is a subring of $\mathbb{Q}$, R is indeed (isomorphic to) a subgroup of frac(R). Inspired by how $n = \frac{n}{1}$, we can show this by the following homomorphism.

$$f(a) = \frac{a}{1_R}$$

We can also show that this system is isomorphic to the construction of adding synthetic units.

For the rest of this chapter, the domains we consider will all be commutative.

5.1 Divisibility in a domain

Divisibility is essentially the same as in number theory.

Definition 5.1 (Divisibility in a commutative domain)**.**

$$x|y \iff \exists r \in D[xr = y]$$

Proposition 5.1.

$$x|y \iff \langle y \rangle \subseteq \langle x \rangle$$

In $\mathbb{Z}$, divisibility is antisymmetric (up to a sign), but this isn't the case in every domain!

Proposition 5.2. Let $u \in D^*$, and $x = uy$, then $x|y$ and $y|x$

The reason why divisibility is antisymmetric in number theory is because ± 1 are the only units in $\mathbb{Z}$.

5.2 GCD in a domain

Definition 5.2 (Greatest common divisor of 2 elements in a domain)**.**

$$d = \gcd(x, y) \iff [r|x \wedge r|y \implies r|d]$$

Let D be a commutative PID, then for every $\langle a, b \rangle = \langle \gcd(a, b) \rangle$

Chapter 6

Associative algebra

Chapter 7

Polynomial rings

Chapter 8

Product Rings

Chapter 9

Modules

Readers are familiar with linear spaces as a field and set where scalar multiplication and vector addition are defined. Typically linear algebra deals with fields on $\mathbb{R}$ or $\mathbb{C}$.

Generalizing the idea of a linear space to be over any ring leads to the idea of a *module*.

Module theory permits the following short and sweet definition for a linear space.

Definition 9.1 (Linear space (Module theory))**.** A *linear space* is a module where the ring is a field.

Part II

Advanced

Chapter 10

Torsion elements

10.1 Annihilators