PMATH 347

Group and Rings

Zhisu Wang
Taught by David McKinnon
University of Waterloo
Spring 2023

Contents

1 Introduction to Groups

1.1 Basic Axioms and Definitions

Definition 1.1

(**Groups**)
A group is an ordered pair $(G, *)$ where G is a set and $*$ is a binary operation on G statisfying the following axioms:

1. (**Associativity**) $(a * b) * c = a * (b * c)$, for all $a, b, c \in G$

2. (**Existence of Identity**) there exists an element 1 in G, called an *identity* of G, such that for all $a \in G$ we have

$$a * 1 = 1 * a = a$$

3. (**Existence of Inverse**) for each $a \in G$, there is an element a^{-1} of G called an *inverse* of a, such that

$$a * a^{-1} = a^{-1} * a = 1$$

Definition 1.2

(**Subgroups**) A subgroup of a group G is a subset $H \subset$ that is also a group using the same operation as G.

Theorem 1.1

(**Subgroup Theorem**)
Let G be a group, $H \subset G$ a nonempty subset. Then H is a subgroup of G if and only if

$$\forall a, b \in H, a \cdot b \in H \text{ and } a^{-1} \in H$$

Definition 1.3

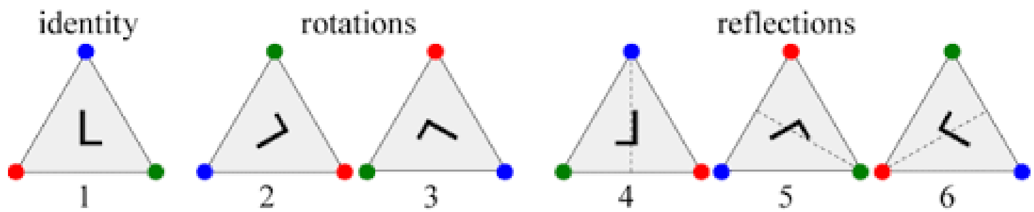
(**Order**)
The order of an element $g \in G$, is the smallest positive integer n satisfying $g^n = 1$.

Definition 1.4

(**Order of groups**)
The order of a group is its cardinalty. Ex: $\mid S_n \mid = n!$

1.2 Dihedral Groups

For each $n \in \mathbb{Z}^+, n \geq 3$, let D_{2n} be the set of symmetries of a regular n-gon, where a symmetry is any rigit motion of the n-gon which can be effected by taking a copy of the n-gon, moving this copt in any fashion in 3-space and then placing the copy back on the original n-gon so it exactly covers it.



An example of D_6

1.3 Symmetric Groups and other groups

Let $n \in \mathbb{N}$, the symmetry group of degree n is a group under function composition $\circ : \{1, \ldots, n\} \to \{1, \ldots, n\}$. In general,

$$\begin{aligned} S_n &= \text{symmetric group on n letters} \\ &= \{\text{permutation of } \{1, \ldots, n\}\} \\ &= \{\text{bijection } f : \{1, \ldots, n\} \to \{1, \ldots, n\}\} \end{aligned}$$

Example 1.0

> How to generate a **disjoint cycle** notation for $G : \{1, \ldots, n\} \to \{1, \ldots, n\}$:
>
> 1. Keep iterating G until yu get back to 1:
>
> $$1, G(1), G(G(1)) \ldots$$
>
> 2. If there are any elements of {1, . . . , n} left, start over at step (1) with the samllest of them.

3. Keep going until you are done.

Example 1.1

(**Other examples of groups**)

1. $\mathbb{Z}/n\mathbb{Z}$:
2. $GL_n(\mathbb{R}) = \{\text{invertible } n \times n \text{ matrices}\}$
3. $SL_n(\mathbb{R}) = \{n \times n \text{ matrices}, det = 1\}$
4. $SO_n(\mathbb{R}) = n \times n$ matrices M, $dist(Mv, Mu) = dist(v, u)$ for all v, u
5. Quaternion Group:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$$

1.4 Homomorhisms and Isomorphisms

Theorem 1.2

This is a theorem.

Proposition 1.3: T

is is a proposition.

1.5 Pictures

Sydney, NSW

2 Introduction to Rings

2.1 Basic Axioms and Definitions

A **ring** is a bunch of things your can add, subtract, and multiply.

Example 2.0

- $\mathbb{Z}$: Integers, $\mathbb{R}$: Real numbers, $\mathbb{Q}$: rationals, $\mathbb{C}$: complex numbers.
- $\mathbb{R}[x, y]$: polynomials in x, y with real coefficients
- $M_n(\mathbb{R})$: $n \times n$ matices with real entries (not commutative)
- $\mathbb{Z}/n\mathbb{Z}$: integers mod n.

Definition 2.1: Ring

A ring is a set R with two operations $+ : R \times R \to R$, $\cdot : R \times R \to R$ satisfying for all $a, b, c \in R$,

1. $(a + b) + c = a + (b + c)$.
2. $a + b = b + a$.
3. There exists $0 \in R$ such that $0 + a = a$.
4. There is a $-a \in R$ such that $a + (-a) = 0$.
5. $(ab) \cdot c = a \cdot (bc)$,
6. There exists $1 \in R$ such that $a \cdot 1 = 1 \cdot a = a$.
7. $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.

Before we prove the subring theorem, here are a couple more defnitions of rings:

Definition 2.2: Commutative Rings

A ring R is commutative **iff** $ab = ba$ for all $a, b \in R$

Definition 2.3: Division Rings

A ring R is a **division ring** iff for all $a \in R, a \neq 0$, there is $a^{-1} \in R$ with $aa^{-1} = a^{-1}a = 1$.

Definition 2.4: Fields

A **field** is a commutative division ring.

Definition 2.5: Unit

An element $a \in R$ is a **unit** iff there is $a^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1$.

Definition 2.6: Zero Divisor

An element $a \in R$ is a **zero divisor** iff $a \neq 0$ and there is some $b \in R, b \neq 0$, with $ab = 0$ or $ba = 0$.

Definition 2.7: Integral Domain

An integral domain, or **domain** is a ring with **no zero divisors**.

$\mathbb{Z}/6\mathbb{Z}$ is not a domain because

$$2 \neq 0, 3 \neq 0, \text{ but}$$

$$2 \cdot 3 = 6 = 0$$

Now we have a theorem:

Theorem 2.1

Every unit is not a zero divisor.

Proof:

Say $a \in R$ is a unit. If $ab = 0$, then $b = a^{-1} \cdot 0 = 0$. If $ba = 0$, then $b = 0 \cdot a^{-1} = 0$. So a is not a zero divisor.

□

We give some examples of units/zero divisors of rings. Consider

- $\mathbb{Z}$: units are $\{1, -1\}$
- $\mathbb{Q}$ is a field, and so are $\mathbb{R}, \mathbb{C}$.
- $M_n(\mathbb{R})$: if $n \geq 2$, $\begin{pmatrix} 0 & \cdots & 0 & 1 \\ 0 & \cdots & 0 & \vdots \\ 0 & \cdots & 0 & 0 \end{pmatrix}^2 = 0$. Units are $GL_n(\mathbb{R})$.
- $\mathbb{R}[x]$: no zero divisors. Units are nonezero constants.

2.2 Subring Theorem

Next, we proceed to the subring theorem so that we don't need to check all axioms of rings.

Definition 2.8: Subring

A **subring** of a ring R is a subset $S \subset R$ that is a ring using the same $+, \cdot$, and 1 as R.

Theorem 2.2: Subring Theorem

A subset $S \subset R$ of a ring R is a subring iff

1. $1 \in S$
2. S is closed under subtraction $-$, that is, $a, b \in S \implies a - b \in S$
3. S is closed under multiplication $\cdot$, that is, $a, b \in S \implies ab \in S$

Proof:

($\Rightarrow$) If S is a subring, then $(1), (2), (3)$ are trivially satisfied.

($\Leftarrow$) So assume S satisfies (1), (2), and (3).
First, note that $\cdot : S \times S \to S$ is well defined by (3).
Since $1 \in S$, by (2), we get $0 = 1 - 1 \in S$, so $-1 = 0 - 1 \in S$.
So if $a, b \in S$, then $-b \in S$ by (3), so $a + b = a - (-b) \in S$, and hence we also have $+ : S \times S \to S$.
Associativity of $+$ and $\cdot$ and commutativity of $+$ are immediately true for S.
Same for distributivity. Existence of 0, additive inverse, and 1 in S follows from (1) and previous discussion.

$\square$

Example: Let $R = \mathbb{C}$, let S be:

$$S = \{a + b\gamma + c\gamma^2 + d\gamma^3 + e\gamma^4 \mid a, b, c, d, e \in \mathbb{Z}, \gamma = e^{\frac{2\pi i}{5}}\}$$

We have $\gamma^5 = 1, \gamma \neq 1$ (We usually write $S = \mathbb{Z}[]$).
By Subring Theorem:

1. $1 \in S$, becasue you can pick $a = 1$, $b, c, d, e = 0$
2. trivial
3. say $x, y \in S$,

$$x = a + b\gamma + c\gamma^2 + d\gamma^3 + e\gamma^4$$

$$y = a' + b'\gamma + c'\gamma^2 + d'\gamma^3 + e'\gamma^4$$

   xy = sum of terms of the form (integers)$\cdot\gamma^n$ for some $n \in \mathbb{Z}_{\geq 0}$. Since $\gamma^5 = 1$, (integer)$\cdot\gamma^n$ can always be written with $n \in \{0, 1, 2, 3, 4\}$.

So S is a subring of $\mathbb{C}$.

2.3 Homomorhisms

Definition 2.9: Homomorphism of Ring

A **homomorphism of rings** is a function $f : R \to T$ such that

1. f(1) = 1
2. $f(ab) = f(a)(b)$
3. $f(a+b) = f(a) + f(b)$

Note: (1) is a must: consider $f(n) = (n, 0)$, we have $f(1)^2 = f(1)$, so it can't be derive with (2).

Definition 2.10: Isomorphism

An **isomorphism** is a homomorphism with an inverse homomorphism.

Theorem 2.3

A homomorphism of rings is an isomorphism **iff** it's a bijection.

Examples of homomorphism:

1. $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $f(a, b) = a$
2. $f : \mathbb{R}[x] \to \mathbb{C}$, where
$$f(p(x)) = p(i)$$
$$f(x^2 + 1) = i^2 + 1 = 0$$
$$f(x^3 + 3x^2 + x - 7) = i^3 + 3i^3 + i - 7 = -10$$
This is a homomorphism, and it's onto.
In fact, plugging stuff in for the variables is always a hom. from a polynomial ring.

Definition 2.11: Image, Kernel

The **image** of a hom. $\phi : R \to T$ is

$$im(\phi) = \{t \in T \mid t = \phi(r) \text{ for some } r \in R\}$$

The **kernel** of ϕ is
$$ker\phi = \{r \in R \mid \phi(r) = 0\}$$

Theorem 2.4

$im\phi$ is a subring of T. $ker\phi$ is not a subring of R.

Proof:

$1 \in Im\phi$ because $1 = \phi(1)$. If $a, b \in Im(\phi)$, then

$$a = \phi(r_1), b = \phi(r_2)$$

so $a - b = \phi(r_1 - r_2) \in Im\phi$ and $ab = \phi(r_1, r_2) \in Im\phi$.
So $Im\phi$ is a subring.
However, if $1 \in ker\phi$, then

$$\phi(1) = 0 \implies \phi(a) = \phi(a)\phi(1) = 0$$

for all $a \in R$, and $\phi(1) = 1$, so $0 = 1$, which is not allowed. So $ker\phi$ is not a subring of R.

□

2.4 R-module

An R-module is a bunch of things you can add, subtract, and multiply by elements of R. Although $ker\phi$ is not a subring of R, it is an **R-module**.

Definition 2.12: R-module

Let R be a ring. An R-module is an abelian group M with a function $\cdot : R \times M \to M$ satisfying:

1. $(r_1 + r_2)m = r_1m + r_2m$
2. $r \cdot (m_1 + m_2) = (r \cdot m_1 + r \cdot m_2)$
3. $r_1 \cdot (r_2 \cdot m) = (r_1r_2) \cdot m$

From now on, every ring we deal with will be commutative.

Example 2.1

- If $R = \mathbb{R}$, then an R-module is exactly the same thing as an $\mathbb{R}$-vector space. In fact, if R is a field, then R-module is exactly the same thing as an R-vector space.
- $2\mathbb{Z} = \{\text{even integers}\}$ is a $\mathbb{Z}$-module.
- $\mathbb{Z}/6\mathbb{Z}$ is a $\mathbb{Z}$-module.

Theorem 2.5: Submodule Theorem

A subset of S of an R-module M is an R-submodule of M iff

1. $0 \in S$
2. S is closed under $-$
3. S is closed under $\cdot$

Proof:

Same as other subxx theorems. $\square$

Definition 2.13: Submodule

A **submodule** of an R-module M is a subset $S \subset M$ that is an R-module using the same operations $+, -, \cdot$ as M.

2.5 Properties of Ideals

Definition 2.14: Ideal

An **ideal** of R is an R-submodule of R.

For example, $2\mathbb{Z}$ is an ideal of $\mathbb{Z}$. We showed last time that if $\phi : R \to T$ is an homomorphism, then $ker\phi$ is an ideal of R. Is is true that every ideal of R is the kernel of some homomorphism.
Answer: YES. Take the quotient. Let's say $I \subset R$ is an ideal. We want to find homomorphism $\phi : R \to T$ with $ker\phi = I$. If we had such a ϕ and such a T, then

$$\phi^{-1}(0) = I$$

$$\phi^{-1}(1) = 1 + I$$

$$\phi^{-1}(t) = r + I$$

where $\phi(r) = t$. So defind R/I to be

$$\{r + I \mid r \in R\}$$

with

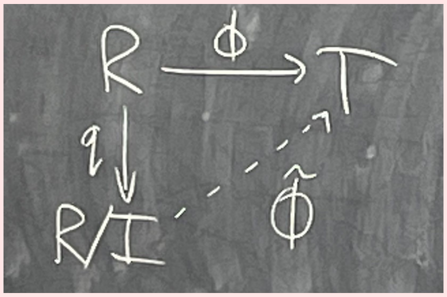
$$(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I$$

$$(r_1 + I)(r_2 + I) = r_1 r_2 + I$$

and $1 + I$ is the mult. identity. It is proven in the textbook that R/I is a ring. R/I is not a subring of R.

Theorem 2.6: Universal Property of Quotients

Let $\phi : R \to T$ be a homomorphism, $I \subset R$ an ideal. Then



there exists a homomorphism $\hat{\phi} : R/I \to T$ statisfying $\phi = \hat{\phi} \circ q$ iff $I \subset ker\phi$.
$q : R \to R/I$ is the reduce mod I homomorphism. Furthermore, $im\hat{\phi} = im\phi$ and $ker\hat{\phi} = q(ker\phi) = ker\phi$ "mod I"

Example 2.2

$\mathbb{R}[x] = \{\text{polys in } x \text{ with real coefficients}\}$
$I = \{p(x) | p(1) = 0\}$ is an ideal.
What does $\mathbb{R}[x]/I$ look like?
Define $\phi : \mathbb{R}[x] \to R$

$$\phi(p(x)) = p(1)$$

so $\phi(x^2 + 1) = 1^2 + 1 = 2$ and $\phi(2x - 7) = 2 - 7 = -5$.
It is easy to see that $ker\phi = I$. Therefore, by the UPQ, $\hat{\phi} : \mathbb{R}[x]/I \to R$ has image $\mathbb{R}$ and kernel 0 mod I. So $\hat{\phi}$ is $1-1$ and onto, so it's an isomorphism. (A ring hom. ϕ is one-to-one iff $ker\phi = \{0\}$).

Theorem 2.7

A ring homomorphism is $1 - 1$ **iff** its kernel is 0.

Proof:

If $\phi : R \to T$ is injective, then $ker\phi = \{0\}$, trivially. So assume $ker\phi = \{0\}$. Say $\phi(a) = \phi(b)$, We want to show $a = b$. Well, $\phi(a - b) = 0$. so $a - b \in ker\phi \Rightarrow a = b$. $\square$

Definition 2.15: Maximal Ideal

An ideal $I \subset R$ is maximal iff $I \neq R$ and if $J \subset R$ is an ideal with $I \subset J \subset R$, then either $J = I$ or $J = R$.

Example 2.3

Let $R = \mathbb{Z}$. What are the ideals of R?
Say $I \subset \mathbb{Z}$ is an ideal. If $I \neq (0)$, then there is some $n \in I, n \neq 0$. Let's choose the smallest positive $n \in I$.
Claim: $I = n\mathbb{Z}$.
Proof of claim: Certainly $n\mathbb{Z}$ is contained in I. We just need to show $I \subset n\mathbb{Z}$. Say $x \in I$. Write

$$x = qn + r$$

where $r, q \in \mathbb{Z}$, $0 \leq r < n$. Then $r = x - qn \in I$. Since $r < n$, we have $r \leq 0$, so $r = 0$. So $x = qn \in n\mathbb{Z}$.

So every ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$. And $n\mathbb{Z} \subset k\mathbb{Z}$ iff $k \mid n$. So $n\mathbb{Z} \subset \mathbb{Z}$ is maximal iff n is prime.

Definition 2.16: Generated Ideal

Let R be a ring, $S \subset R$ be any subset. The **ideal generated** by S the intersection of all ideals that contains S. It's written as (S).
More concretely,

$$(S) = \{r_1 s_1 + \ldots + r_n s_n \mid r_i \in R, s_i \in S\}$$

When $S = \{x\}$, then

$$(x) = \{rx \mid r \in R\}$$

Example 2.4

1. $(1) = R$
2. $(6, 8) \subset \mathbb{Z}$.

   $$(6, 8) = \{a6 + b8 \mid a, b \in \mathbb{Z}\}$$

   We know this is (n) for some $n \in \mathbb{Z}$. Since $2 = 8 - 6 \in (6, 8)$ we have $(2) \subset (6, 8)$. But $6, 8 \in (2)$, so $(6, 8) \subset (2)$, so $(6, 8) = (2)$.

Theorem 2.8

An ideal $I \subset R$ is maximal **iff** R/I is a field.

Proof:

We'll start by proving

Lemma 2.9

The ideals of R/I are precisely the reductions mod I of ideals of R that contain I.

Proof:

Say $J \subset R$ is an ideal with $I \subset J$. Then if $q : R \to R/I$ is the quotient homomorphism, $q(J)$ is an ideal of R/I because homs. map ideals to ideals.
Conversely, if $\bar{J}$ is an ideal of R/I, define

$$J = \{r \in R \mid q(r) \in J\} = q^{-1}(J)$$

This is an ideal: $0 \in J$ since $q(0) = 0 \in \bar{J}$.
If $x, y \in J$, then

$$q(x - y) = q(x) - q(y) \in \bar{J}$$

so $x - y \in J$.
If $r \in R$ and $x \in J$, then we want $rx \in J$. But $q(rx) = q(r)q(x) \in \bar{J}$, so $rx \in J$.
Finallly, note that if $x \in I$, then $q(x) = 0 \in \bar{J}$, so $x \in J$.
Moreover, if $\bar{J}_1 \neq \bar{J}_2$, then $J_1 \neq J_2$ because q is onto. $\square$

($\Rightarrow$) R/I is a field. We want to show that $I \subset R$ is maximal. First, note that any ideal that contains a unit must be the whole ring. Any nonzero ideal of R/I contains a unit, so it's R/I. (If $a \in I$ is a unit, then $\frac{1}{a}(a) \in I$, so $1 \in I$, so $r \cdot 1 \in I$ for all $r \in R$). So R/I has 2 ideals, R/I and (0). So by the lemma, the only ideals of R that contains I are I and R. So I is maximal.

($\Leftarrow$) Conversely, assume I is maximal. We want to show that R/I is a field. By the lemma, R/I has exactly 2 ideals, (0) and R/I. Let $x \in R/I$ be any nonzero element. Then $(x) = R/I$, so $1 = rx$ for some $r \in R/I$. So x is a unit, and R/I is field. $\square$

The maximal ideals of $\mathbb{Z}$ are the ideals (p) for p prime. So $\mathbb{Z}/n\mathbb{Z}$ is a field **iff** n is prime.

Example 2.5

Say F is a field. What are the maximal ideals of $F[x]$? First, say $I \subset F[x]$ is an ideal. We could have $I = (0)$. If not, then there is some $p(x) \in I$ for $p(x) \neq 0$. Let $p(x) \in I$ for $p(x) \neq 0$. Let $p(x)$ be a nonzero polynomial of minimal degree. We'll show $I = (p(x))$. Say $q(x) \in I$, we want to show $q(x) = t(x)p(x)$ for some $t(x) \in F[x]$.

$$q(x) = t(x)p(x) + r(x)$$

where $deg(r(x)) < deg(p(x))$. But $r(x) = q(x) - t(x)p(x) \in I$, so by minimality of $deg(p)$, we have $r(x) = 0$ and

$$q(x) = t(x)p(x)$$

so $I = (p(x))$.

We proved R/I is a field **iff** I is a maximal ideal **iff** R/I has only two ideals (0) and (1).

Theorem 2.10

Let $\phi : F \to T$ be a homomorphism, where F is a field. Then ϕ is injective.

Proof:

$ker\phi$ is an ideal of F. So $ker\phi = (0)$ or (1). But $\phi(1) = 1 \neq 0$. So $ker\phi = (0)$. □

Reminder: A domain is a ring with no zero divisors; that is, if $ab = 0$, then $a = 0$ or $b = 0$. So R/I is a domain iff $ab \equiv 0 \text{ mod } I \implies a \equiv 0 \text{ mod } I$ or $b \equiv 0 \text{ mod } I$ iff $ab \in I \implies a \in I$ or $b \in I$.

Definition 2.17: Prime Ideal

An ideal $I \subset R$ is prime iff for all $a, b \in R$ with $ab \in I$, either $a \in I$ or $b \in I$.

Theorem 2.11

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

Proof:

We just did it. □

Example 2.6

What are the prime ideals of $\mathbb{Z}$? $n\mathbb{Z} = (n)$ is maximal iff n is prime. $n\mathbb{Z}$ is prime iff n is prime or $n = 0$.

2.6 Principal Ideal Domain

Definition 2.18: Principal Ideal Domain

A principle ideal domain is a domain D such that every ideal of D can be generated by one element.

Example 2.7

1. $\mathbb{Z}$ is a PID.

2. $F[x]$, F is a field, x a variable, is a PID.

Let R be any ring. There is a unique hom. $\phi : \mathbb{Z} \to R$, called the characteristic homomorphism, defined by

$$\phi(n) = \begin{cases} \underbrace{1 + 1 + \ldots + 1}_{\times n} & n \geq 0 \\ \underbrace{-(1 + 1 + \ldots + 1)}_{\times -n} & n < 0 \end{cases}$$

The kernel of ϕ is $n\mathbb{Z}$ for some $n \in \mathbb{Z}$, we might as well assume $n \geq 0$, because $n\mathbb{Z} = -n\mathbb{Z}$. The value of n is called the characteristic of R.

Example 2.8

1. If $R = \mathbb{Z}$, then $\text{char}\mathbb{Z} = 0$, because the characteristic hom. is the identity hom. which is $1 - 1$.

2. If $R = \mathbb{Q}$, $\text{char}\mathbb{Q} = 0$

3. $\mathbb{Z}/n\mathbb{Z}$ has characteristic n.

4. $\mathbb{Z}/3\mathbb{Z}[x]$ has characteristic

facts: If D is a domain then $im\phi$ is also a domain. So $ker\phi$ is a prime ideal of $\mathbb{Z}$, so $\text{char}D = 0$ or prime (converse if not true!).

Let's say R is a ring, T a ring that contains R, $\alpha \in T$ some element. Then

$$R[\alpha] = \{a_n\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0 \mid a_i \in R, n \in \mathbb{Z}\}$$

Example 2.9

1. $\mathbb{Z}[\zeta_5], \zeta_5 = e^{\frac{2\pi i}{5}}$.

$$\begin{aligned}\mathbb{Z}[\zeta_5] &= \{a_n\zeta_5^n + \ldots + a_0 \mid a_i \in \mathbb{Z}\}\\ &= \{a_0 + a_1\zeta_5 + a_2\zeta_5^2 + a_3\zeta_5^3 + a_4\zeta_5^4 + a_5\zeta_5^5 \mid a_i \in \mathbb{Z}\}\end{aligned}$$

$$x_5 + 1 \to 2(x = \zeta_5)$$

$$x + 1 \to 1 + \zeta_5(x = \zeta_5)$$

2. $\mathbb{Z}[i]$

$$\begin{aligned}\mathbb{Z}[i] &= \{a_n i^n + \ldots + a_0 \mid a_i \in \mathbb{Z}\}\\ &= \{a_1 i + a_0 \mid a_1 \in \mathbb{Z}\}\end{aligned}$$

3. $\mathbb{Z}[\sqrt{2}, \sqrt{3}]$.

$$\begin{aligned}\mathbb{Z}[\sqrt{2}, \sqrt{3}] &= \{p(\sqrt{2}, \sqrt{3}) \mid p(x,y) \text{ polynomials with coefficients in } \mathbb{Z}\}\\ &= \{a_0 + a_{10}\sqrt{2} + a_{01}\sqrt{3} + a_{11}\sqrt{6}\}\end{aligned}$$

Quiz 8:
The ideal of $(p(x))$ is maximal iff there are no ideals T with $p(1) \subsetneq J \subsetneq F[x]$. But $(p(x)) \subset (q(x))$ iff $q(x) \mid p(x)$, so $(p(x))$ is maximal iff $p(x)$ has no nontrivial factors in $F[x]$.

Definition 2.19: Irreducible

A polynomial $p(x) \in F[x]$ is irreducible iff $p(x)$ is not constant and has no nontrivial factors.

so $(p(x))$ is maximal iff $(p(x))$ is irreducible. $(p(x))$ is prime iff $p(x)$ is irreducible or 0.
Note: Two different polynomials can represent the same function. x^3 and x represents the same function in $\mathbb{F}_3[x]$, but they are different polynomial ($\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$).

2.7 Properties of R-modules

If F is a field, then an F-module is an F-vector space.

Definition 2.20: R-module Homomorhisms

An R-module **homomorphism** is a function $\phi : M \to N$, where M, N are R-modules satisfying

1. $\phi(rm) = r\phi(m)$
2. $\phi(m_1 + m_2) = \phi(m_1) + \phi(m_2)$

Example 2.10

1. An F-module homomorphism is an F-linear transformation if F is a field.
2. $R = \mathbb{Z}$, $\phi : \mathbb{Z}_{12} \to \mathbb{Z}_3$ such that
$$\phi(n) = n \mod 3$$
3. $\phi : \mathbb{Z}^2 \to \mathbb{Z}^2$ such that
$$\phi(a, b) = (a + b, a - b)$$
This is a $\mathbb{Z}$-module homomorphism. It's 1-1 but not onto.