Part I

Rings

1 Introduction

With groups, the motivation is symmetries. What motivates rings?

- Numbers
- Algebraic Geometry
  Any ring becomes a ring of functions on something.
  Algebra $\iff$ Geometry
- Arithmetic Geometry
  Arithmetic Geometry is most closely related to number theory.
- Functions on some space

Definition. A ring $R$ is a set with two binary operations, normally denoted $+$ and $\times$, that satisfy the following axioms:

1. $(R, +)$ is an Abelian group. In particular, it has a 0 element.
2. Associativity under multiplication: $(ab)c = a(bc)$
3. Distributivity: $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.

In essence, a ring is an Abelian group under addition, a monoid under multiplication, and the two operations are related through distributivity.

We don’t require a multiplicative identity, but most rings we will consider have one. Such a ring is called a ring with identity or ring with unity. Also if the multiplication operation is commutative, we call $R$ a commutative ring.

One asks very different questions about commutative and noncommutative rings. In 611, 99% of rings will be commutative and will have a multiplicative identity. We will see some examples of noncommutative rings, but no theory.

Basic Examples: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{H} = \mathbb{R}1 + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k$

In the last example, the $i, j, k$ are the elements from the quaternions, $\mathbb{Q}_8$, and are related by $i^2 = j^2 = k^2 = ijk = -1$. It is necessary to check associativity to verify that $\mathbb{H}$ is, in fact, a ring. In general, however, one can check distributivity first and then check associativity on generators. In the case of $\mathbb{H}$, this is still quite a bit of work, and we will present an alternative proof later.

More Examples:

- $\mathbb{Z}/n\mathbb{Z}$ is a ring under “modular arithmetic”.

- If $X$ is any set, and $R$ is a ring, then $R^X :=$ the set of all functions from $X \to R$ is a ring.
  The operations are given by pointwise addition, $(f + g)(x) := f(x) + g(x)$, and pointwise multiplication, $(fg)(x) := f(x)g(x)$.

- If $X$ is a topological space, and $R = \mathbb{R}$, then $\mathcal{C}(X, \mathbb{R})$ (the continuous functions $X \to \mathbb{R}$) is a subring of $R^X$.

- Infinitely differentiable functions, $C^\infty((a, b), \mathbb{R})$, is a ring.

- More generally, we have $C^\infty(X, \mathbb{R})$ where $X$ is a smooth manifold.
2 Vocab

- **Subring**: $S$ is a subring of $R$ if $S$ is an Abelian subgroup of $R$ and $S$ is closed under multiplication. Check that $\forall a, b \in S$, $a - b \in S$ and $ab \in S$.

- **Zero-divisor**: $a \in R$, $a \neq 0$ such that $\exists b \in R : ab = 0$, $b \neq 0$.
  Ex. $\mathbb{Z}/6\mathbb{Z}$, $3 \cdot 2 \equiv 6 \equiv 0$ (mod $6$) so these are zero divisors.

- **(Integral) domain**: a commutative ring with $1 \neq 0$ with no zero divisors.

- **Unit**: $a \in R$, such that $\exists b \in R : ab = ba = 1$.
  For this to make sense, $R$ needs to have $1$. These are the invertible elements in the ring.

- **$R^\times$, Group of Units**: the group formed by the set of all units of $R$ under multiplication.

- **Division Ring**: a ring $R$ with $1 \neq 0$ such that every nonzero element has an inverse. In other words, $R - \{0\} = R^\times$.
  Ex. $\mathbb{H}$, since $(a + bi + cj + dk)^{-1} = \frac{a-bi-cj-dk}{a^2+b^2+c^2+d^2}$.

- **Field**: a commutative division ring. There is a multiplicative identity, every element has an inverse, and multiplication is commutative. In other words, $R - \{0\}$ is an Abelian group under multiplication.
  Ex. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields.

3 Constructions of Rings

3.1 Mat$_n(R)$, rings of matrices

$R$ is a ring. Mat$_n(R) = n \times n$ matrices. If $A = (a_{ij}), B = (b_{ij}) \in$ Mat$_n(R)$, define addition component-wise, so $(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij})$ where the addition operation is performed as in the ring. Define matrix multiplication in the typical way, so that $(a_{ij})(b_{ij}) = (\sum_{k=1}^n a_{ik}b_{kj})$, and again the operations on each element are performed as defined in the ring. We must check that this is, in fact, a ring.

by verification. There is an embedding of $\mathbb{H} \hookrightarrow \text{Mat}_2(\mathbb{C})$, by the “Pauli matrices”:

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

Therefore we can conclude that $\mathbb{H}$ is associative. (This is the proof alluded to in the basic examples of section 1.)

3.2 Product ring

$R_1$ and $R_2$ are rings. The product ring is the set $R_1 \times R_2 = \{(r_1, r_2) : r_1 \in R_1, r_2 \in R_2\}$ under component-wise operations. $R_1 \times R_2$ has an identity if and only if $R_1$ and $R_2$ have an identity, in which case it is $(1_1, 1_2)$. $R_1$ and $R_2$ are (isomorphic to) subrings of $R_1 \times R_2$.

The identity in a subring need not be the identity of an ambient ring. For instance, $\mathbb{Z}$ is a ring, and $2\mathbb{Z}$ is a subring which does not even contain the identity. A cheap example of a case where a subring has a different multiplicative identity is when you consider the trivial subring $\{0\}$. It would be nice to have a different example, however.

The definition in class given for subring was actually that $S$ is a subring if there is an embedding of $S$ in $R$. In this case note that above $R_1$ is definitively a subring of $R_1 \times R_2$. This isn’t entirely clear to me, since the book’s definition and the definitions I found online are not of this form, and the discussion which follows involving idempotents is related to this idea.

Let $i : S \hookrightarrow R$, where $S, R$ are rings with $1$. Then $i(1_S) = e$ for some $e \in R$. We have $i(1_S)^2 = i(1_S \cdot 1_S) = i(1_S)$, so $e^2 = e$, and therefore $e$ is idempotent. If $R$ is a domain, then $e = 0$ or $1$. 
3.3 $R[x]$, rings of polynomials

$R[x] = \{a_0 + a_1x + \cdots + a_dx^d : a_i \in R\}$ is a ring under component-wise addition and formal multiplication:

$$\sum_{i=0}^{d} a_i x^i \sum_{j=0}^{e} b_j x^j = \sum_{i=0}^{d} \sum_{j=0}^{e} a_i b_j x^{i+j}.$$ 

$R[x]$ has an identity, the constant 1 polynomial. We can also generalize to the ring of power series $R[[x]]$, where multiplication is defined as

$$\sum_{i=0}^{\infty} a_i x^i \sum_{j=0}^{\infty} b_j x^j = \sum_{k=0}^{\infty} \left( \sum_{i+j=k} a_i b_j \right) x^k.$$ 

This is an associative ring, and $R[x] \hookrightarrow R[[x]]$. In general, $R[x]$ cannot be thought of as a function $R \to R$, for example consider $x^p - x \in \mathbb{Z}_p[x]$. By Fermat’s Little Theorem, $a^p \equiv a \pmod{p} \Rightarrow a^p - a \equiv 0 \forall a \in \mathbb{Z}_p$ so $x^p - x$ is the zero polynomial.

4 Homomorphisms of Rings

A homomorphism of rings is a function $\varphi : R \to S$ such that

1. $\varphi$ is a homomorphism of $R$ and $S$ as Abelian groups.

2. $\varphi(ab) = \varphi(a)\varphi(b) \quad \forall a, b \in R.$

If $1 \in R$, then $\varphi(1)\varphi(1) = \varphi(1) \Rightarrow \epsilon^2 = \epsilon$, so $\varphi(1)$ is always an idempotent element but not necessarily the identity.

$\text{Ker } \varphi = \{ r \in R : \varphi(r) = 0 \}$, so it is the kernel of the group homomorphism. For this reason, $\text{Ker } \varphi$ is an Abelian subgroup of $R$. If $a, b \in \text{Ker } \varphi$, $\varphi(ab) = \varphi(a)\varphi(b) = 0$ so it is a subring. Note that it was not necessary for both $a, b$ to be in $\text{Ker } \varphi$, it is enough for only one of them to be. This gives us the motivation for the definition of the ideal of a ring. After we define it, we will see that $\text{Ker } \varphi$ is a two-sided ideal of $R$.

**Definition.** A right/left/two-sided ideal $I$ is a subset of $R$ such that

1. $I$ is an Abelian subgroup.

2. (Right) $a \in I, b \in R \Rightarrow ab \in I$. So $I$ is closed under right-multiplication by elements of $R$.

   (Left) $a \in I, b \in R \Rightarrow ba \in I$. So $I$ is closed under left-multiplication by elements of $R$.

   (Two-Sided) $a \in I, b \in R \Rightarrow ab, ba \in I$. So $I$ is closed under multiplicative conjugation by elements of $R$.

If $R$ is commutative, then all three types of ideals are the same.

**Lemma 1.** The image of a ring homomorphism $\varphi : R \to S$ is a subring of $S$

**Proof.** $\varphi(R)$ is an Abelian subgroup of $S$ by group theory. If $a, b \in \varphi(R)$ then for some $x, y \in R$, $\varphi(x) = a$ and $\varphi(y) = b$ so $\varphi(xy) = \varphi(x)\varphi(y) = ab$ and hence $ab \in R$.

**Examples:**

1. $\mathbb{Z} \xrightarrow{\epsilon} \mathbb{Z}/n\mathbb{Z}$ by “reduction modulo $n$”.

   $\text{Ker } \varphi = n\mathbb{Z}$.

2. $C[0,1] \xrightarrow{\epsilon} R, \varphi(f) = f(\frac{1}{2})$, the “evaluation map”, which sends a function to it’s value at $\frac{1}{2}$.

   $\text{Ker } \varphi = \{ f : f(\frac{1}{2}) = 0 \}$.
5 Quotient Rings

$R$ is a ring, $I \subseteq R$ is a two-sided ideal. The quotient ring $R/I$ is

1. $R/I$ as the (Abelian) quotient group.

2. Multiplication defined by $(a + I)(b + I) = (ab + I)$

We must check that this is well defined:

\[
\begin{align*}
    a + I &= a' + I, & b + I &= b' + I \\
    a' &= a + x, b' = b + y & \text{where } x, y \in I \\
    (a' + I)(b' + I) &= a'b' + I = ab + xb + ay + xy + I = ab + I
\end{align*}
\]

So $R/I$ is well defined as a ring. We also have a homomorphism $R \rightarrow R/I$ defined by $\pi(a) = a + I$.

**Theorem 1.** (First Isomorphism Theorem) Let $\varphi : R \rightarrow S$ be a homomorphism. Then $R/\ker \varphi \cong \varphi(R)$.

**Proof.** The two are isomorphic as groups from the previous group theory work. Now let $I = \ker \varphi$ and $\pi : R/I \rightarrow \varphi(R)$ be defined by $\pi(a + I) = \varphi(a)$, which is the same function which establishes the group isomorphism. This is therefore a bijective map, so the only thing to verify is that it is a ring homomorphism:

\[
\varphi((a + I)(b + I)) = \varphi(ab + I) = \varphi(ab) = \varphi(a)\varphi(b) = \pi(a + I)\pi(b + I).
\]

\[\square\]

The second isomorphism theorem is not used much.

**Theorem 2.** (Third Isomorphism Theorem) Let $I \subseteq R$ be a two-sided ideal.

1. There is a bijection between the ideals of $R$ which contain $I$ and the ideals of $R/I$

2. For any two-sided ideal $J$ of $R$ containing $I$ we have $R/J \cong \frac{R/I}{J/I}$

**Proof.** (1.) Let $J$ be an ideal containing $I$, and let $J$ get mapped to $\pi(J) \cong J/I$, where $\pi$ is the canonical homomorphism from $R \rightarrow R/I$. Then take any $a \in \pi(J)$, $b \in R/I$. Then there is some $x \in J$ such that $\pi(x) = a$, and some $y \in R$ such that $\pi(y) = b$. Then $ab = \pi(x)\pi(y) = \pi(xy)$, but since $J$ is an ideal $xy \in J$ and therefore $ab \in \pi(J)$, so $\pi(J)$ is an ideal. Now let $K$ be an ideal of $R/I$. Then take $a \in \pi^{-1}(K)$, and $b \in R$. Then $\pi(ab) = \pi(a)\pi(b)$, but since $\pi(a) \in K$ and $K$ is an ideal we have that $\pi(a)\pi(b) \in K$ and so $\pi(ab) \in \pi^{-1}(K)$ so $\pi^{-1}(K)$ is an ideal.

(2.) Define $\varphi : R/I \rightarrow R/J$ as $\varphi(a + I) = a + J$. First we prove that this is well defined: $a + I = a' + I \Rightarrow a = a' + i$ for some $i \in I$. Then since $I \subseteq J$, $i \in J$ and therefore $a + J = a' + J$. Now we prove it is a homomorphism:

\[
\begin{align*}
    ((a + I) + (b + I)) &= \varphi(a + b + I) = a + b + J = (a + J) + (b + J) = \varphi(a + I) + \varphi(b + I) \\
    \varphi((a + I)(b + I)) &= \varphi(ab + I) = ab + J = (a + J)(b + J) = \varphi(a + I)\varphi(b + I)
\end{align*}
\]

Finally, note that $\varphi(a + I) = J$ iff $a \in J$ iff $a + I \in J/I$, thus $\ker \varphi = J/I$ and therefore the result follows by the First Isomorphism Theorem (for rings). \[\square\]

6 Ideals

**Definition.** For $a \in R$,

- $aR = \{ax \mid x \in R\}$ is a right ideal
- $Ra$ defined similarly is a left ideal
- $RaR$ is the minimal two-sided ideal containing $a$.
- If $R$ is commutative, $aR = Ra = RaR = (a)$ is the principal ideal generated by $a$.

More generally, for $\{a_i\} \subseteq R$ where $R$ is commutative, then minimal ideal containing all the $\{a_i\}$ is the set of finite linear combinations $\{\sum r_i a_i\}$ where the $r_i \in R$ and only finitely many $r_i$ are nonzero.
6.1 Operations with Ideals

Let $I, J \subseteq R$ be ideals.

- $I + J = \{x + y \mid x \in I, y \in J\}$ is an ideal.
- $I \cap J$ is an ideal.
- $IJ = \{\sum r_i x_i y_i \mid r_i \in R, x_i \in I, y_i \in J\}$ is an ideal.

Note: $IJ \subseteq I$ and $IJ \subseteq J$ so $IJ \subseteq I \cap J$, but not necessarily equal: $(4)(6) = (24)$, but $(4) \cap (6) = (12)$.

Going forward, all rings will be commutative with identity unless otherwise specified.

**Definition.** An ideal $I \subseteq R$ is called maximal if $I \neq R$ and if $I \subseteq J \subseteq R$ where $J$ is an ideal, then $J = I$ or $J = R$.

**Lemma 2.** Any ideal $I \subseteq R$ is contained in a maximal ideal.

To prove this we need Zorn’s Lemma, so first we give some background. Given a set with a partial ordering, $(S, \leq)$, i.e. we have that for $a, b, c \in S$ which can be compared (it is not required that we can compare all elements of $S$) that

- $a = b \iff a \leq b$ and $b \leq a$
- $a \leq b$ and $b \leq c \Rightarrow a \leq c$.

An element $a \in S$ is called maximal if $b \geq a \Rightarrow b = a$. Take any subset $T \subseteq S$. An upper bound for $T$ is an element $a \in S$ such that $a \geq x$ for all $x \in T$. A sequence of elements $a_1 \leq a_2 \leq \ldots$ is called a chain.

**Zorn’s Lemma:** If every chain has an upper bound then $S$ has a maximal element.

Let’s use this axiom to prove the previous lemma.

**Proof.** Let $S$ be the set of ideals such that $I \subseteq J$, and $J \neq R$. Then let $J_1 \subseteq J_2 \subseteq \ldots$ be a chain, and now take $J = \bigcup J_i$. We need to prove that $J$ is in $S$, because if it is then every chain has an upper bound, which will complete our proof.

First let’s prove that $J$ is an Abelian group. Let $a, b \in J$. Then $a \in J_{m_1}$ and $b \in J_{m_2}$ for some $m_1, m_2 \in \mathbb{N}$, but then we have that $a - b \in J_{\max(m_1, m_2)}$, thus $a - b \in J$. Now take $a \in J$, $r \in R$. Then $a$ is in some $J_N$, and therefore $ar \in J_N$ which means that $ar \in J$ and hence $J$ is an ideal. Finally, we need to prove that $J \neq R$. Note that an ideal is equal to the ring if and only if it contains 1. Now suppose $1 \in J$, then $1 \in J_N$ for some $N \in \mathbb{N}$, but then $J_N = R$ which is a contradiction, hence $J \neq R$.

Therefore every chain has an upper bound, so $S$ has a maximal element $M$. This $M$ is an ideal which contains $I$ but is not $R$. Now assume $A$ is an ideal such that $M \subseteq A \subseteq R$. If $A$ is not $R$ then $A$ also contains $I$, so $A \in S$ and since $M$ is maximal we have that $A \subseteq M$ which implies that $A = M$. Thus $M$ is maximal.

**Fact** $R$ is a field iff $R$ has no proper ideals.

**Proof.** If $R$ is a field, then consider an ideal $I$ which contains some nonzero element $a$. Then $aa^{-1} \in I$, but then $1 \in I$ and therefore $I = R$. Hence $R$ contains no proper ideals.

Now suppose $R$ contains no proper ideals. Then consider the ideal $I$ generated by some nonzero element $a$. Since this ideal is not proper, but it is not just the zero ideal, we have that $I = R$ and hence there is some element of $R$ such that $ar = 1$. Hence $a$ is invertible, and since $a$ was arbitrary $R$ is a field.

**Corollary 1.** An ideal $I$ is maximal iff $R/I$ is a field.

**Proof.** $R/I$ is a field if and only if it has no proper ideals. By the third isomorphism theorem for rings, there is a bijection between ideals if $R/I$ and ideals of $R$ containing $I$, thus $R/I$ is a field iff there are no proper ideals of $R$ containing $I$ except $I$ itself, which is the definition of a maximal ideal.
**Definition.** An ideal \( I \subseteq R \) is called prime if \( I \neq R \) and for \( x, y \in R \), if \( xy \in I \Rightarrow x \in I \) or \( y \in I \).

Example: \((2) \subseteq \mathbb{Z} \), since \( xy \) is even iff \( x \) is even or \( y \) is even.

**Theorem 3.** An ideal \( I \subseteq R \) is prime iff \( R/I \) is an integral domain.

**Corollary 2.** Maximal ideals are prime, because any field is a domain.

**Proof.** (\( \Rightarrow \)) Let \( I \) be prime, and suppose \((x + I)(y + I) = I\). Then \( xy + I = I \), so \( xy \in I \) from which we know that \( x \in I \) or \( y \in I \), and therefore there are no zero divisors (since \( I \) is zero in \( R/I \)).

(\( \Leftarrow \)) Suppose \( R/I \) is an integral domain. Then for \( x, y \in R \) such that \( xy \in I \), we have that \( xy + I = I \), that is \((x + I)(y + I) = 0\). Since \( R/I \) is an integral domain, we have that either \( x \in I \) or \( y \in I \), thus \( I \) is prime. \(\square\)

**Definition.** Ideals \( I \) and \( J \subseteq R \) are called coprime (also sometimes called comaximal) if \( I + J = R \).

Note that this is true iff there are \( x \in I \), \( y \in J \) such that \( 1 = x + y \).

Example: \((2) + (3) = \mathbb{Z} \), since \(-2 + 3 = 1\).

**Theorem 4. Chinese Remainder Theorem:** If \( I \) and \( J \) are coprime ideals then:

1. \( IJ = I \cap J \)
2. \( R/IJ \cong R/I \times R/J \)

Example: \((2)(3) = (6) = (2) \cap (3) \), and \( \mathbb{Z}/(6) \cong \mathbb{Z}/(2) \times \mathbb{Z}/(3) \). The latter part says that for any \( a, b \in \mathbb{Z} \) there is an \( n \in \mathbb{Z} \) such that \( n \equiv a \pmod{2} \) and \( n \equiv b \pmod{3} \).

**Proof.** (1) We already had that \( IJ \subseteq I \cap J \), so take \( a \in I \cap J \). Then, letting \( x + y = 1 \) be elements \( x, y \in I, J \) respectively, which exist since \( I \) and \( J \) are coprime, we have that \( a = ax + ay \in IJ \). Hence \( I \cap J \subseteq IJ \), and therefore \( IJ = I \cap J \).

(2) Consider the homomorphism \( \varphi : R \to R/I \times R/J \) defined as \( \varphi(x) = (x + I, x + J) \). First let’s verify that this is a homomorphism:

\[
\varphi(x + y) = (x + y + I, x + y + J) = (x + I, x + J) + (y + I, y + J) = \varphi(x) + \varphi(y) \\
\varphi(xy) = (xy + I, xy + J) = (x + I, x + J)(y + I, y + J).
\]

Now \( \varphi(x) = (I, J) \) iff \( x \in I \) and \( x \in J \), i.e. \( \ker \varphi = I \cap J = IJ \). Now on the other hand, for any \( (a + I, b + J) \in R/I \times R/J \), starting with \( x + y = 1 \) where \( x, y \in I \), we have that \( a - b = x(a - b) + y(a - b) \) and then let \( z = a - x(a - b) = b + y(a - b) \). Then \( \varphi(z) = (a + I, b + J) \), so the map is surjective. Hence by the first isomorphism theorem we have that \( R/IJ \cong R/I \times R/J \). \(\square\)

**Theorem 5. Generalized Chinese Remainder:** Let \( I_1, I_2, \ldots, I_k \subseteq R \) be pairwise coprime ideals (\( I_i + I_j = R \) for any \( i \neq j \)).

1. \( I_1I_2 \cdots I_k = I_1 \cap I_2 \cap \cdots \cap I_k \)
2. \( R/(I_1 \cdots I_k) \cong R/I_1 \times \cdots \times R/I_k \)

**Proof.** From the previous specific case, it holds for \( k = 2 \). We proceed by induction on \( k \); suppose it holds for \( k - 1 \), that is \( I_1 \cdots I_{k-1} = I_1 \cap \cdots \cap I_{k-1} \) and \( R/I_1 \cdots I_{k-1} \cong R/I_1 \times \cdots \times R/I_{k-1} \). Now since \( I_k \) is coprime to each \( I_j \) for \( j \in \{1, \ldots, k - 1\} \), we have some element \( x_j \in I_j \) and \( y_j \in I_k \) for each \( j \) such that \( x_j + y_j = 1 \). Then \( \prod_{j=1}^{k} (x_j + y_j) = 1 = \prod_{j=1}^{k} x_j + y \) where \( y \in I_k \), since each term other than the first is multiplied by some element of \( I_k \). Note as well that \( \prod_{j=1}^{k} x_j \in I_1 \cap \cdots \cap I_{k-1} \), so \( I_1 \cdots I_{k-1} \) and \( I_k \) are coprime.

Now by what we’ve already done for the specific form of the CRT, \( I_1 \cdots I_{k-1} I_k = I_1 \cdots I_{k-1} \cap I_k = I_1 \cap \cdots \cap I_k \) and \( R/(I_1 \cdots I_{k-1})I_k \cong R/(I_1 \cdots I_{k-1}) \times R/I_k \cong R/I_1 \times \cdots \times R/I_k \). \(\square\)
7  ED, PID, and UFD

What do we like about \( \mathbb{Z} \)?

1. (ED) Division with remainder
2. (PID) Greatest common divisor, \((a, b) = ax + by\)
3. (UFD) Unique factorization

Plan: Prove that ED \( \subseteq \) PID \( \subseteq \) UFD.

7.1 ED - Euclidean Domains

**Definition.** A domain \( R \) is called **Euclidean** if there exists a function \( N : R \setminus \{0\} \to \mathbb{Z}_{\geq 0} \) (called the **norm**) such that \( \forall a, b \in R, \) where \( b \neq 0, \) either \( a = bq \) or \( a = bq + r \) with \( N(r) < N(b) \).

**Examples:**

- \( \mathbb{Z}, N(x) = |x| \)
- \( k[x] \) where \( k \) is a field, \( N(f) = \deg f \) (long division)
- Gaussian integers \( \mathbb{Z}[i] = \{ a + bi | a, b \in \mathbb{Z} \} \).

**Claim.** The Gaussian integers, \( \mathbb{Z}[i] \), is a Euclidean domain.

**Proof.** Let \( N(a + bi) = a^2 + b^2 \). Then take \( \alpha, \beta \in \mathbb{Z}[i] \) where \( \beta \neq 0 \). If \( \alpha = \beta \gamma \) for some \( \gamma \in \mathbb{Z}[i] \), we are done. If not, draw \( (\beta) \), which is a square tiling of the plane where each square has a side length \( |\beta| \), and each vertex is \( \beta \gamma \) for some \( \gamma \in \mathbb{Z}[i] \). Then \( \alpha \) is inside one of the squares, and we choose \( \gamma \) such that \( \beta \gamma \) is the closest vertex to \( \alpha \). Now \( N(\alpha - \beta \gamma) < N(\beta) \iff |\alpha - \beta \gamma| < |\beta| \) since \( N(x) = |x|^2 \), and the latter inequality holds because any point \( \alpha \) will be strictly inside the circle centered at \( \beta \gamma \) with radius \( |\beta| \). \( \square \)
7.2 PID - Principal Ideal Domains

Definition. A domain $R$ is called a Principal Ideal Domain (PID) if all ideals $I \subseteq R$ are principal, i.e. $I = (x)$ for some $x \in I$.

Theorem 6. Any ED is a PID.

Proof. Let $R$ be an ED with norm $N$, and let $I \subseteq R$ be an ideal. Then take $d \in I$ to be an element with least norm (which makes sense, since $N : R \to \mathbb{Z}_{\geq 0}$). Now take any element $a \in I$, then $a = qd + r$ where $r = 0$ or $N(r) < N(d)$. Therefore $r = a - qd \in I$, but $d$ was an element of $I$ with least norm, so $r$ must be 0. Therefore $a = qd$, and since $a$ was arbitrary we have that $I = (d)$.

Corollary 3. $\mathbb{Z}$, $k[x]$, and $\mathbb{Z}[i]$, are PIDs.

7.2.1 Divisibility in Commutative Rings

For $a, b \in R$, TFAE

1. $a = bq$
2. $(a) \subseteq (b)$

In this case we say that $b$ divides $a$, or that $b$ is a divisor of $a$.

Definition. Let $R$ be a domain, and choose nonzero $a, b \in R$. TFAE

1. $(a) = (b)$
2. $a = bu$ where $u$ is a unit
3. $b = au'$ where $u'$ is a unit

In this case we say that $a$ and $b$ are associated.

Definition. Let $R$ be a domain, and $a, b \in R$. The greatest common divisor (gcd) of $a$ and $b$ is $d \in R$ such that $d|a$, $d|b$, and $d$ is divisible by any other common divisor of $a$ and $b$.

Remark: The gcd($a, b$) does not always exist, but if it does then it is unique up to association, since if $d$ and $d'$ are both gcd($a, b$) then $d|d'$ and $d'|d$ so $(d) = (d')$.

Lemma 3. For $a, b \in R$, suppose $(a, b) = (d)$. Then $d = \gcd(a, b)$. In particular, if $R$ is a PID then gcd($a, b$) always exists, and gcd($a, b$) = $ax + by$ for some $x, y \in R$.

Proof. Suppose $(a, b) = (d)$. Then $(a) \subseteq (d)$ and $(b) \subseteq (d)$. Now suppose $(a) \subseteq (d')$ and $(b) \subseteq (d')$, then $a = d'u$ and $b = d'v$ for some $u, v \in R$, and so $(a, b) \subseteq (d')$ but then $(d) \subseteq (d')$, hence $d$ is the gcd($a, b$).

Remark: In a Euclidean Domain $R$, gcd($a, b$) can be found by the Euclidean Algorithm.

7.3 UFD - Unique Factorization Domain

Definition. $R$ is a commutative ring with identity. Then for any nonunit $a \in R$, $a$ is called reducible or composite if $a = xy$ and neither $x$ nor $y$ is a unit. If this is not possible, then $a$ is called irreducible.

Definition. A domain $R$ is called a Unique Factorization Domain (UFD) if

1. Any element $a \in R$ is either a unit or we can write $a = x_1 \cdots x_n$ where each $x_i$ is irreducible.
2. If $a = x_1 \cdots x_n = y_1 \cdots y_m$ where each $x_i$ and $y_i$ is irreducible, then $n = m$ and $\exists \sigma \in S_n$ such that $x_i$ and $y_{\sigma(i)}$ are associated.
How to check existence of factorization: Take \( a \in R \), where \( a \) is not a unit. If \( a \) is irreducible, then we are done. Otherwise, \( a = xy \) where neither \( x \) nor \( y \) are units. Repeat this process recursively with \( x \) and \( y \). If the algorithm terminates, then we have a factorization. If this algorithm does not terminate, then we can find a sequence of elements \( a_1, a_2, \ldots \) such that \( a_n | a_{n-1} \) (i.e. \( a_{n-1} \subseteq (a_n) \)) and \( a_n \) and \( a_{n-1} \) are not associated. Thus we have a chain of principal ideals:

\[
(a_1) \subseteq (a_2) \subseteq \cdots
\]

**Definition.** Let \( R \) be a commutative ring with identity. \( R \) is called Noetherian if any increasing chain of ideals in \( R \) stabilizes. That is, if

\[
I_1 \subseteq I_2 \subseteq \cdots \subseteq R \implies \exists n : I_n = I_{n+1} = \cdots = R.
\]

**Proposition.** If \( R \) is a Noetherian domain then factorization into irreducibles exists.

**Proposition.** Any PID is Noetherian.

**Proof.** Let \( R \) be a PID. We argue by contradiction, suppose we have

\[
I_1 \subsetneq I_2 \subsetneq \cdots
\]

and let \( I = \bigcup_{i=1}^{\infty} I_i \). This is a union of nested ideals, so it is itself an ideal (see the proof that any ideal \( I \subsetneq R \) is maximal). Since \( R \) is a PID, \( I = (x) \) for some \( x \in I \). Thus \( x \in I_n \) for some \( n \in \mathbb{N} \), so \( (x) \subseteq I_n \). On the other hand, we have

\[
I_n \subsetneq I_{n+1} \subsetneq I_{n+2} \subsetneq \cdots \subseteq I = (x) \subseteq I_n
\]

which is a contradiction. \( \square \)

**Lemma 4.** (Euclid’s Lemma) If \( R \) is a PID and \( x \in R \) is a nonunit, then \( x \) is irreducible if and only if \( (x) \) is a prime ideal.

**Proof.** Suppose \( (x) \) is a prime ideal. Then if \( x = ab \) for some \( a, b \in R \), either \( a \in (x) \) or \( b \in (x) \). But then \( a = xu \Rightarrow x = xu(b) = 1 = ub \) or \( b = xu \Rightarrow x = x(u) = 1 = au \) for some \( u \in R \), so at least one of \( a \) or \( b \) is a unit and thus \( x \) is irreducible.

Now suppose \( x \) is irreducible. Then take \( a, b \in R \) and suppose \( ab \in (x) \). Now consider \( (a, x) = (d) \), since \( R \) is a PID. Thus \( a = da' \) and \( x = dx' \), but then either \( d \) is a unit or \( x' \) is a unit. In the second case, we would have that \( x = x'^{-1} a' \) and thus \( a \in (x) \). On the other hand if \( d \) is a unit then there are \( u, v \in R \) such that \( au + xv = 1 \) and then since \( ab = xc \) we can write \( abu + xbv = b = x(au + bv) \), thus \( b \in (x) \). \( \square \)

**Lemma 5.** Suppose \( R \) is a domain such that

1. Factorization into irreducibles exist
2. \( R \) has the property that \( x \) is irreducible iff \( (x) \) is a prime ideal

then \( R \) is a UFD. In particular, if \( R \) is a PID it is a UFD.

**Proof.** Suppose \( a \in R \) and \( a = x_1 \cdots x_n = y_1 \cdots y_m \) where \( x_i \) and \( y_i \) are irreducible. Let’s argue by induction on \( \max(n, m) \). Obviously for \( \max(n, m) = 1 \) we have \( x_1 = y_1 \), so the desired conclusion holds. Now suppose it holds for \( \max(n, m) = k \), and wlog suppose \( n = k + 1 \) while \( m \leq k \). Then \( y_1 \cdots y_m \in (x_{k+1}) \), so \( y_1 \in (x_{k+1}) \) or \( y_2 \cdots y_m \in (x_{k+1}) \). By recursion here at most \( m \) times, one of the \( y_i \in (x_{k+1}) \). Thus \( y_i = x_{k+1}u_i \), where \( u_i \in R \) must be a unit since \( y_i \) is irreducible, and therefore \( (x_{k+1}) = (y_i) \). We therefore have

\[
x_1 \cdots x_{k+1} = y_1 \cdots y_{i-1} y_{i+1} \cdots y_m x_{k+1} u_i \implies x_1 \cdots x_k = y_1 \cdots y_{i-1} y_{i+1} \cdots y_m u
\]

by cancellation. Therefore the result follows from our induction hypothesis. \( \square \)

Map of the rings: Interesting rings in Algebra are typically Noetherian.

\[\text{Insert picture here}\]
Math 611 - Abstract Algebra

Rings

Notes from lectures by Jenia Tevelev

**Definition.** Let $R$ be a commutative ring with identity. The spectrum of the ring, $\text{spec } R$, is the set of its prime ideals.

Example: $\text{spec } \mathbb{Z} = \{(p) : p \in \mathbb{Z} \text{ is prime or 0}\}$

What is $\text{spec } \mathbb{Z}[i]$? Since the Gaussian integers are a PID, we know that $(x)$ is a prime ideal iff $x$ is irreducible, so what are the irreducible Gaussian integers? For instance, are the primes in $\mathbb{Z}$ irreducible? No - consider $2 = (1 + i)(1 - i)$.

**Theorem 7.** (Fermat) For any prime $p \in \mathbb{Z}$, TFAE

1. $p = x^2 + y^2$ for some $x, y \in \mathbb{Z}$
2. $p = 2$ or $p \equiv 1 \pmod{4}$
3. $-1$ is a square in $\mathbb{Z}/p\mathbb{Z}$
4. $p$ is reducible in $\mathbb{Z}[i]$

**Proof.**

$(1) \Rightarrow (2)$ Let $p = x^2 + y^2$ for some $x, y \in \mathbb{Z}$. Note that for any $x \in \mathbb{Z}$, $x^2 \equiv 0, 1 \pmod{4}$ since these are the only squares in $\mathbb{Z}/4\mathbb{Z}$. Thus $x^2 + y^2 \equiv 0, 1, 2 \pmod{4}$. However, since $p = x^2 + y^2$ is prime, we are done - if $p \equiv 2 \pmod{4}$ we must have that $p = 4k + 2$, so in order for $p$ to be prime $k = 0$ and thus $p = 2$. If $p \equiv 0 \pmod{4}$ then $p = 4k$, which is a contradiction, hence $p = 2$ or $p \equiv 1 \pmod{4}$.

$(2) \Rightarrow (3)$ If $p = 2$ then $-1 \equiv 1^2 \pmod{2}$. Now if $p \equiv 1 \pmod{4}$ then $p = 4k + 1$, and so we are considering $-1 \in \mathbb{Z}/(4k+1)\mathbb{Z}$ as a ring. Consider just the multiplicative structure of such a ring, which is therefore isomorphic to $\mathbb{Z}/4k\mathbb{Z}$. The multiplicative order of $-1$ is 2, so it must be mapped to an element of $\mathbb{Z}/4k\mathbb{Z}$ of order 2. The element $2k$ is the only element of this latter group of order 2. Then let $x$ be the element mapped to $k$. Since $\phi(x^2) = 2\phi(x) = 2k = \phi(-1)$, we have that $x^2 \equiv -1 \pmod{p}$ where $\phi : (\mathbb{Z}/p\mathbb{Z})^* \rightarrow \mathbb{Z}/4k\mathbb{Z}$.

$(3) \Rightarrow (4)$ If $-1$ is a square in $\mathbb{Z}/p\mathbb{Z}$, then there exists some $x \in \mathbb{Z}/p\mathbb{Z}$ such that $x^2 \equiv 1 \pmod{p}$, or rather $x^2 = kp - 1$. Then $kp = (x+i)(x-i)$. Suppose $p$ is irreducible. Then since $\mathbb{Z}[i]$ is a UFD we know that $(x+i) \subseteq (p)$ or $(x-i) \subseteq (p)$. In the first case, we have for some $a, b \in \mathbb{Z}$ that $x+i = p(a+bi) \Rightarrow pb = 1$ which is a contradiction. Similarly we find that $x-i = p(a+bi) \Rightarrow -1 = pb$ which is a contradiction. Hence $p$ is reducible in $\mathbb{Z}[i]$.

$(4) \Rightarrow (1)$ If $p$ is reducible in $\mathbb{Z}[i]$ that means that $p = zw$ for some nonunits $z, w \in \mathbb{Z}[i]$. Thus $N(p) = N(zw) = N(z)N(w) \Rightarrow p^2 = N(z)N(w)$ where $N(z)$ and $N(w)$ are not 1 (since $z, w$ are nonunits) and therefore $p = N(z) = N(w) = x^2 + y^2$ for some $x, y \in \mathbb{Z}$.

**Lemma 6.** Take any homomorphism $\varphi : A \rightarrow B$ of rings. Suppose $I \subseteq B$ is a prime ideal. Then $\varphi^{-1}(I)$ is a prime ideal of $A$. This gives a map from $\text{spec } B \rightarrow \text{spec } A$.

**Proof.** Suppose $x, y \in A$ and $xy \in \varphi^{-1}(I)$. Then $\varphi(xy) \in I$ but then $\varphi(x)\varphi(y) \in I$ and since $I$ is prime we know that $\varphi(x)$ or $\varphi(y)$ are therefore in $I$, hence $x$ or $y$ are in $\varphi^{-1}(I)$.

**Theorem 8.** (Lagrange) Any positive integer is the sum of 4 squares.

**Proof.** Sketch of proof: Look at the Gaussian Quaternions, $\mathbb{H}_\mathbb{Z} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{Z}\}$. Then $N(z) = z\bar{z} = a^2 + b^2 + c^2 + d^2$. Also, the norm is multiplicative since $\overline{zw} = \overline{w}\overline{z}$, and this yields $N(zw) = zw\overline{zw} = z\overline{w}\overline{z} = zN(w)\overline{z} = z\overline{z}N(w) = N(z)N(w)$. This yields the corollary that if $a, b$ are the sum of four squares then $ab$ is also. Hence it suffices to prove Lagrange’s theorem for primes.

Is $\mathbb{H}_\mathbb{Z}$ a PID? It’s not commutative, so this doesn’t really make sense, but we can ask if any right ideal is principal. If $I \subseteq \mathbb{H}_\mathbb{Z}$ is a right ideal, take a nonzero $x \in I$ which has the smallest norm. Then, as with Gaussian Integers, $I$ breaks $\mathbb{R}^4$ into hypercubes with sides of length $|x| = \sqrt{N(x)}$. 

\[\text{Spec picture here} \]
Is it true that the distance from any point of the cube to one of its vertices is less than the length of the side? Well the diagonal of this hypercube has length $2|x|$, so the center is not going to work. In order to fix this, enlarge the ring to Hurwitz Quaternions:

$$\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{Z} \text{ or } a, b, c, d \in \frac{1}{2} + \mathbb{Z}\}$$

In this ring any right ideal is principal. \qed

8 Rings of Polynomials

All rings are commutative with identity, and we consider the ring of polynomials $R[x]$.

Reminder: If $k$ is a field then $k[x]$ is an Euclidean Domain, and therefore a PID and UFD.

Theme: If $R$ has a good property then $R[x]$ typically has good properties.

Theorem 9. If $R$ is a domain then $R[x]$ is a domain.

Proof. Let $R$ be a domain, and let $f, g \in R[x]$ be polynomials defined as

$$f(x) = a_nx^n + \cdots + a_0, \quad g(x) = b_mx^m + \cdots + b_0,$$

where $a_n, b_m$ are nonzero. One way to do this would be to note that $a_0b_0 = 0$ implies that $a_0 = 0$ or $b_0 = 0$. Then we can factor $x$ out of $fg - a_0b_0$, and the result follows by induction on $n + m$. A faster way is as follows.

Consider the leading term of $fg$, which is $a_nb_mx^{n+m}$. The coefficient must be zero, hence $a_n = 0$ or $b_m = 0$ since $R$ is a domain, but this is a contradiction. \qed

The trick in general is to use the constant or leading terms, often the leading terms work better.

8.1 Noetherian Inheritance

Theorem 10. (Hilbert’s Basis Theorem) If $R$ is Noetherian then $R[x]$ is Noetherian.

Reminder: $R$ is Noetherian if every ascending chain of ideals in $R$ stabilizes.

Lemma 7. $R$ is Noetherian if and only if every ideal of $R$ is finitely generated.

Proof. ($\Rightarrow$) We prove the contraposition: suppose that $I$ is an ideal which is not finitely generated. Pick $a_1 \in I$, and let $I_1 = (a_1)$. Then pick $a_i \in I \setminus I_{i-1}$, and let $I_i = (\{a_1, \ldots, a_i\})$. Then $I_1 \subsetneq I_2 \subsetneq \cdots$ is a chain of ideals which does not stabilize, so $R$ is not Noetherian.

($\Leftarrow$) Suppose that every ideal of $R$ is finitely generated, and let $I_1 \subsetneq I_2 \subsetneq \cdots$ be a chain of ideals. (Since these are each proper subsets, they can never stabilize.) Then $I = \bigcup_{i=1}^\infty I_i$ is an ideal (since the $I_i$ are nested) and therefore it is finitely generated, say $I = (\{a_1, \ldots, a_n\})$. Now each $a_1$ must be in one of the $I_i$, say that $a_i \in I_{k_i}$, then let $N = \max\{k_1, \ldots, k_n\}$. Then we have that $I_1 \subsetneq \cdots \subsetneq I_N \subsetneq I \subsetneq I_N$ which is a contradiction, hence $R$ is Noetherian. \qed

Now we can prove Hilbert’s Basis Theorem.

Proof. Let $R$ be a Noetherian ring. Take $I \subseteq R[x]$, and let’s show that $I$ has finitely many generators using the trick of inspecting the leading terms. Let $J \subseteq R$ be the set of leading terms of all polynomials in $I$ (include zero as the leading term of the zero polynomial, for instance). We now show that $J$ is an ideal.

Take $a, b \in J$. Then there are polynomials $f = ax^n + \cdots + a_0$ and $g = bx^m + \cdots + b_0$ in $I$, and then

$$fx^m - gx^n = (a - b)x^{n+m} + \cdots \in I$$

so $a - b \in J$ and therefore $J$ is a subgroup of $R$. Now assuming $a \in J$, we have that $f = ax^n + \cdots + a_0$ is in $I$ and therefore so is $rf = (ra)x^n + \cdots + (ra_0)$ for any $r \in R$, hence $ra \in J$. Therefore $J$ is an ideal of $R$. 

11
Since \( R \) is Noetherian, \( J \) is finitely generated, that is \( J = (\{a_1, \ldots, a_n\}) \). Choose polynomials \( f_i \in I \) such that the leading term of \( f_i \) is \( a_i \), and let \( F_0 \) be the set of the \( f_i \). Let \( N = \max(\deg(f_i)) \). We now claim that for any \( f \in I \), we have that \( f = g + h \) where \( g \in (\{f_1, \ldots, f_n\}) \) and \( \deg(h) < N \), and we will prove this by induction on \( \deg(f) \). For \( \deg(f) = 0 \) it is true easily: if \( N = 0 \) then \( h = 0 \), since \( f \) is a constant polynomial and so it’s leading coefficient is a member of \( J \), and when \( N = 0 \) then \( J = (\{a_1, \ldots, a_n\}) = (\{f_1, \ldots, f_n\}) \). If \( N \neq 0 \) then \( 0 < N \) so we can just take \( h = f \).

Now assume it holds for all polynomials of degree less than \( f \). If \( \deg f < N \) then just take \( h = f, g = 0 \), so suppose \( \deg(f) \geq N \). Then let \( f = ax^m + \cdots + a_0 \), and so \( a = \sum_{i=1}^{n} r_i a_i \) for some \( r_i \in R \). Then \( ax^m + \text{l.o.t.} = \sum_{i=1}^{n} r_i f_i x^{m-\deg f_i} = \overline{g} \), and therefore \( f - \overline{g} \) has degree less than \( f \), and by our induction hypothesis we can write \( f - \overline{g} = g + h \Rightarrow f = \overline{g} + g + h \) where \( \overline{g} + g \in (\{f_1, \ldots, f_n\}) \) and \( \deg h < N \).

Now let \( J_k \subseteq R \) to be the set of leading terms of all polynomials in \( I \) of degree \( k \) for \( k = 0, \ldots, N - 1 \). Then \( J_k \) is an ideal, and each \( J_k \) is finitely generated, say \( J_k = (\{b^{(k)}_1, \ldots, b^{(k)}_n\}) \). Then take polynomials \( f_i^{(k)} \in I \) of degree \( k \) with leading term \( b_i \), and let \( F_k \) be the set of the \( f_i^{(k)} \). The final claim is that \( \sum_{i=0}^{N-1} F_i = I \).

Take any \( f \in I \), and write it as \( f = g + h \) where \( g \in (F_0) \) and \( \deg h < N \). Then let \( h = bx^k + \text{l.o.t.} \) and therefore for some lower order terms we can generate \( bx^n + \text{l.o.t.} = \overline{h} \in (F_k) \). Then \( h - \overline{h} \) has degree less than \( h \), and for degree 0 it terminates, thus we are done by recursion.

\[ \square \]

### 8.2 UFD Inheritance (Gauss Lemma)

**Theorem 11.** If \( R \) is a UFD then \( R[x] \) is also a UFD.

**Plan:**

1. First construct the field of fractions \( F \) of \( R \).
2. \( F[x] \) is always a UFD since \( F \) is a field.
3. Compare factorization in \( R[x] \) with factorization in \( F[x] \) (Gauss Lemma).

#### 8.2.1 Field of Fractions

\( R \) can be any domain. Goal: construct a field \( F \) which contains \( R \). For example, \( \mathbb{Z} \hookrightarrow \mathbb{Q} \).

Construction: Consider pairs \( (a, b) \) with \( b \neq 0 \), and \( a, b \in R \). We want these to be “fractions,” \( \frac{a}{b} \). Define an equivalence relation:

\[
(a, b) \sim (a', b') \iff ab' = a'b
\]

**Things to check:**

1. Check that it is an equivalence relation
2. Define addition and multiplication
3. Show that these definitions are well defined
4. Show that \( F \) is a ring (check associativity, distributivity)
5. Show that \( F \) is a field
6. Show that there is an embedding \( R \hookrightarrow F \), specifically \( r \mapsto \frac{r}{1} \)

---

12
8.3 Gauss Lemma

**Definition.** A polynomial \( f \in R[x] \) is called **primitive** if the gcd of all its coefficients is equal to 1.

For instance, any monic polynomial is primitive.

**Theorem 12.** (Gauss Lemma - Take 1) Let \( R \) be a UFD, then if \( f, g \in R[x] \) are primitive, \( fg \) is primitive.

**Proof.** Argue by contradiction. Suppose \( f, g \in R[x] \) are primitive, but \( fg \) is not. Then the coefficients of \( fg \) have a common divisor which is not a unit, and since \( R \) is a UFD we know that there is therefore some irreducible \( p \) which divides all coefficients of \( fg \). Also, since \( R \) is a UFD then \( (p) \) is a prime ideal. (This was proved in a homework problem.) Therefore we have that \( R/(p) \) is an integral domain.

Now consider the homomorphism \( R[x] \to R/(p)[x] \) which sends \( f = \sum a_i x^i \mapsto \bar{f} = \sum (a_i + (p))x^i \). Then \( \bar{f} \bar{g} = \bar{f}g = 0 \iff \bar{f} = 0 \) or \( \bar{g} = 0 \) because \( R/(p) \) is an integral domain, but this is a contradiction and hence we must have that \( fg \) is primitive.

\( \square \)

**Theorem 13.** (Gauss Lemma - Take 2) Let \( R \) be a UFD, \( f \in R[x] \), and \( F \) be the field of fractions of \( R \). If \( f \) is reducible in \( F[x] \) then it is also reducible in \( R[x] \).

**Proof.** Suppose \( f \) is reducible in \( F[x] \), say \( f = gh \) where \( g, h \in F[x] \). Let \( g = \alpha g' \) and \( h = \beta h' \) where \( \alpha, \beta \in F \) and \( g', h' \in R[x] \) are primitive (we are simply taking common denominators for all terms, and pulling out any common divisors). Then \( f = gh = \alpha \beta g'h' = \gamma f' \) where \( \gamma = \alpha \beta \in F \) and \( f' = g'h' \in R[x] \) is primitive. Let \( \gamma = \frac{s}{t} \) for \( r, s \in R \), then \( sf = rf' \). Then \( r \) is the gcd of the coefficients on the right. Since \( s \) divides the coefficients on the left, we must have that \( s \mid r \) and therefore \( \gamma \in R \). Hence \( f = \gamma g'h' \) is the reduction of \( f \) in \( R[x] \).

\( \square \)

**Corollary 4.** (Gauss Lemma - Take 3) Let \( R \) be a UFD, and \( f \in R[x] \) be irreducible. Then either

- \( \deg f = 0 \) and \( f \in R \) is irreducible
- or

- \( \deg f > 0 \), \( f \) is primitive, and \( f \) is irreducible as an element of \( F[x] \)

**Theorem 14.** (Gauss Lemma - Take 4) If \( R \) is a UFD, then \( R[x] \) is a UFD.

**Proof.** **Existence:** Take any reducible \( f \in R[x] \), and we will show that it can be written as the product of irreducibles. If \( \deg f = 0 \) then it can be written as a product of irreducibles in \( R \) since \( R \) is a UFD. Now suppose all reducible polynomials of degree less than \( f \) can be written as a product of irreducibles. First write \( f = \alpha f' \) where \( f' \in R[x] \) is primitive and \( \alpha \in R \) can be further reduced into irreducibles. Now if \( f' \) is irreducible we are done, if not we have \( f' = gh \) for some non units \( g, h \in R[x] \). Then we must have that \( \deg(g) \) and \( \deg(h) \) are greater than zero, for otherwise \( f' \) would not be primitive. Therefore since \( \deg(gh) = \deg(g) + \deg(h) = \deg(f) \), both \( g \) and \( h \) must have degree strictly less than \( f' \). The result therefore follows by induction.

**Uniqueness:** Suppose we have

\[
\alpha_1 \cdots \alpha_n f_1 \cdots f_s = \beta_1 \cdots \beta_m g_1 \cdots g_t
\]

where each \( \alpha_i, \beta_i \in R \) is irreducible and each \( f_i, g_i \in R[x] \) are primitive irreducible polynomials. Then by the Gauss Lemma - Take 1, \( f_1 \cdots f_s \) and \( g_1 \cdots g_t \) are primitive, so we must have that \( \alpha_1 \cdots \alpha_n = u\beta_1 \cdots \beta_m \) where \( u \in R \) is a unit. Uniqueness of this expression follows from the fact that \( R \) is a UFD, so we can turn our focus to the polynomials.

We now have that \( f_1 \cdots f_s = ug_1 \cdots g_t \) by using association and cancellation of the elements of \( R \). Since \( f_i, g_j \) are irreducible in \( R[x] \) they must also be irreducible in \( F[x] \) (Gauss Lemma - Take 3), but then since \( F[x] \) is a UFD we find that \( s = t \) and that \( f_i \) is associated to \( g_{\sigma(i)} \) for some \( \sigma \in S_n \) in \( F[x] \). It remains to show that \( f_i \) and \( g_{\sigma(i)} \) are associated in \( R[x] \). Now,

\[
f_i = \frac{r}{s} g_{\sigma(i)} \implies sf_i = r g_{\sigma(i)},
\]

and by primitivity we have that \( s \mid r \) (and \( r \mid s \)), so \( \frac{s}{r} \in R \) (and \( \frac{r}{s} \in R \)) and hence \( (f_i) = (g_{\sigma(i)}) \) in \( R[x] \) as well. \( \square \)
9 Polynomials - Roots and Irreducibility Criterion

Throughout this section, \( k \) is a field.

Example: \( x - a \) is irreducible for any \( a \in k \), because if \( a \neq b \) then \( (x - a) \neq (x - b) \) as ideals.

**Lemma 8.** For \( f(x) \in k[x] \), TFAE:

1. \( f(a) = 0 \)
2. \( f(x) = (x - a)g(x) \)

**Proof.** \( (2) \Rightarrow (1) \):

\[
\begin{align*}
\text{Let's do long division:} \\
f(x) &= (x - a)g(x) + r(x) \\
f(a) &= (a - a)g(a) + r(a) = r(a) \\
\text{Thus, } f(x) &= (x - a)g(x)
\end{align*}
\]

\( (1) \Rightarrow (2) \) Let's do long division:

\[
\begin{align*}
f(x) &= (x - a)g(x) + r(x) & \text{where deg } r < \text{deg}(x - a) \Rightarrow r \text{ is constant} \\
f(a) &= 0 = (a - a)g(a) + r(a) = r(a) \Rightarrow r(x) = 0 \\
\therefore f(x) &= (x - a)g(x)
\end{align*}
\]

**Corollary 5.** For \( \deg f < 4 \), if \( f(x) \) is reducible then \( f(x) \) has a root.

This bound is sharp - \( (x^2 + 1)^2 \in \mathbb{R}[x] \) is reducible, but has no roots.

**Corollary 6.** If \( \deg f = d \) then \( f(x) \) has at most \( d \) roots.

**Proof.** Each root gives a linear factor. Since \( k[x] \) is a UFD it can have at most \( d \) irreducible linear factors.

**Application:** The lemma above can help us prove the following theorem.

**Theorem 15.** If \( \Gamma \subset k^\times \) is a finite subgroup of \( k^\times \) then \( \Gamma \) is cyclic.

Examples:

- \( F_p^\times \cong \mathbb{Z}_{p - 1} \) where \( p \) is prime.
- More generally if \( F_q \) is a finite field then \( F_q^\times \cong \mathbb{Z}_{q - 1} \).
- \( \Gamma \subset \mathbb{C}^\times \) is finite \( \implies \Gamma = \mu_n \) for some \( n \) (here \( \mu_n \) is the group of the \( n \)th roots of unity, i.e. \( \mu_n = \{z \in \mathbb{C} : z^n = 1\} \)).

**Lemma 9.** Let \( \Gamma \) be any finite Abelian group written multiplicatively, and let the period of \( \Gamma \) be defined as \( \text{per}(\Gamma) = \min\{n : x^n = 1 \forall x \in \Gamma\} \). Then

1. \( \text{per}(\Gamma) \) divides \( |\Gamma| \)
2. \( \text{per}(\Gamma_1 \times \Gamma_2) = \text{lcm}(\text{per}(\Gamma_1), \text{per}(\Gamma_2)) \)
3. \( \text{per}(\Gamma) = |\Gamma| \) if and only if \( \Gamma \) is cyclic

How does this lemma imply the previous theorem? Let's assume the lemma is true, and offer a proof of the theorem:

**Proof.** Let \( \Gamma \subset k^\times \) be a finite subgroup. Let \( n = \text{per}(\Gamma) \). Then \( x^n = 1 \forall x \in \Gamma \). That is, \( x^n - 1 \) has at least \( |\Gamma| \) roots. By corollary 6 it can have at most \( n \) roots, so \( |\Gamma| \leq n \). Since \( n||\Gamma| \) by (the assumed) lemma 9, we have \( |\Gamma| = n \). Lemma 9 also implies that \( \Gamma \) is cyclic.

Now let’s prove the lemma we just assumed.
Proof. (1) For any \( x \in \Gamma \), we have that \( x^{\mid \Gamma \mid} = 1 \) by Lagrange’s Theorem, thus \( \text{per}(\Gamma) \leq \mid \Gamma \mid \). Also, \( (\Gamma) \) is the lcm of the orders of elements \( x \in \Gamma \). Since \( \mid x \mid \) divides \( \mid \Gamma \mid \) then the lcm of the orders divides \( \mid \Gamma \mid \) as well.

(2) Recall that \( \text{ord}(x) = \text{lcm}(\mid x \mid, \mid y \mid) \). Now \( \text{per}(\Gamma_1 \times \Gamma_2) = \text{lcm}(\text{ord}(x), \text{ord}(y)) \) where the right is taken over all \( x \in \Gamma_1 \) and all \( y \in \Gamma_2 \), but this is the same as taking \( \text{lcm}(\text{lcm}(\text{ord}(x)), \text{lcm}(\text{ord}(y))) = \text{lcm}(\text{per}(\Gamma_1), \text{per}(\Gamma_2)) \).

(3) First note that \( \leftarrow \) is obvious. Now for the \( \Rightarrow \) implication, assume \( \Gamma = \prod \mathbb{Z}_{p_i^{k_i}} \) where the \( p_i \) are primes with possible repetitions. In this case, we have \( \text{per}(\Gamma) = \text{lcm}(p_i^{k_i}) \). By assumption, however, we have that \( \text{per}(\Gamma) = \prod p_i^{k_i} \), and in order for this to be equal to \( \text{lcm}(p_i^{k_i}) \) we must have that \( p_i^{k_i} \) and \( p_j^{k_j} \) are coprime for all \( i \neq j \), that is \( p_i \neq p_j \). Therefore, by the Chinese Remainder Theorem, \( \prod \mathbb{Z}_{p_i^{k_i}} \cong \mathbb{Z}_{\prod p_i^{k_i}} \), so \( \Gamma \) is cyclic. \( \square \)

Lemma 10. A field \( k \) is algebraically closed if one of the following equivalent conditions are satisfied:

1. Any polynomial \( f(x) \in k[x] \) of degree \( > 0 \) has a root
2. Any polynomial \( f(x) \) of positive degree can be factored into a product of linear polynomials
3. Any maximal ideal of \( k[x] \) has a form \( (x - a) \) for \( a \in k \)
4. All prime ideals are described by \( k[x] = \{0\} \cup_{a \in k} \{(x - a)\} \)

Remark: (3) is similar to the description of maximal ideals in \( C[0,1] \).

Example: \( \mathbb{C} \) is an algebraically closed field (Fundamental Theorem of Algebra).

Irreducible polynomials in \( \mathbb{R}[x] \):

1. Linear: \( x - a \) for \( a \in \mathbb{R} \)
2. Quadratic: \( (x - a)(x - \overline{a}) \) where \( a \in \mathbb{C} \setminus \mathbb{R} \)

Proposition 1. Any irreducible polynomial in \( \mathbb{R}[x] \) is of type (1) or (2).

Proof. Take an irreducible polynomial \( f(x) \in \mathbb{R}[x] \). If \( \deg f = 1 \) then it is of type (1). If \( \deg f > 1 \) then it has a complex root \( a \in \mathbb{C} \setminus \mathbb{R} \) (since otherwise it would be reducible by lemma 8). Then note that \( f(\overline{a}) = \overline{f(a)} \) because \( f \) has real coefficients, and therefore \( f(\overline{a}) = 0 \), so we have \( f(x) = (x - a)(x - \overline{a})g(x) \). Since \( f \) is irreducible \( g \) is a constant, so \( f \) is of type (2). \( \square \)

Example: \( f(x) = x^2 + x + 1 \in \mathbb{F}_2[x] \), then since \( f(0), f(1) \neq 0 \) corollary 5 implies that \( f \) is irreducible in \( \mathbb{F}_2[x] \).

Then \( \langle x^2 + x + 1 \rangle \) is a maximal ideal, and \( \mathbb{F}_2[x]/\langle x^2 + x + 1 \rangle \) is a field with elements \( \{0, 1, I, x + I, x + 1 + I\} \cong \mathbb{F}_4 \).

How did we know, before identifying the elements of \( \mathbb{F}_2[x]/\langle x^2 + x + 1 \rangle \), that it was a field?

Theorem 16. (Rational Roots Theorem) Let \( R \) be a UFD, \( F \) the field of fractions, \( f(x) = a_nx^n + \cdots + a_0 \in \mathbb{R}[x] \). Then if \( f(\frac{a}{b}) = 0 \) for \( a, b \in R \) (and in a UFD we may assume it is in lowest terms, i.e. \( \gcd(a, b) = 1 \)), we must have \( a|a_0 \) and \( b|a_n \).

Proof. Write

\[
\begin{align*}
a_n\left(\frac{a}{b}\right)^n + \cdots + a_0 &= 0 \\
a_n a^n + \cdots + a_0 b^n &= 0
\end{align*}
\]

and therefore \( a \) must divide \( a_0 \) and \( b \) must divide \( a_n \) since we are in a UFD and \( \gcd(a, b) = 1 \). \( \square \)

Example: \( x^3 + 3x + 1 \) is irreducible over \( \mathbb{Z} \), because the only possible rational roots are \( \pm 1 \) but neither works.

Theorem 17. (Eisenstein’s Criterion) Let \( R \) be a UFD, and \( p \in R \) be an irreducible element. Take \( f(x) = a_nx^n + \cdots + a_0 \in \mathbb{R}[x] \). If

- \( p \nmid a_n \)
- \( p \mid a_i \) for all \( i < n \)
\begin{itemize}
\item $p^2 \nmid a_0$
\end{itemize}

then $f(x)$ cannot be written as a product of two non-constant polynomials in $R[x]$.

**Proof.** Suppose $f(x)$ is reducible, so $f(x) = g(x)h(x)$ where $g,h \in R[x]$. Let’s “reduce mod $p$”, i.e. consider the quotient ring $R/(p)$, and the homomorphism $R[x] \to R/(p)[x]$ which takes $f \mapsto \overline{f}$ as in theorem 12 (essentially take each coefficient of $f$ mod $p$). Then $\overline{f}(x) = \overline{g}(x)\overline{h}(x)$, and $f(x) = \overline{a}_n x^n$. Let $b_i$ and $c_j$ be the first terms of $g$ and $h$ respectively which are not 0 mod $p$, then $\overline{g}(x) = \overline{b}_ix^i + \text{h.o.t.}$ and $\overline{h}(x) = \overline{c}_jx^j + \text{h.o.t.}$ so we have that the lowest degree nonzero term of $\overline{g}(x)\overline{h}(x)$ is $\overline{b}_i\overline{c}_j x^{i+j}$. (Note: $\overline{b}_i\overline{c}_j$ is nonzero because $R/(p)$ is an integral domain.)

Now this implies that $i+j = n$. Now if $g$ and $h$ are not constant, we have that $i,j > 0$ so $\overline{g}(x) = \overline{b}_ix^i$ and $\overline{h}(x) = \overline{c}_jx^j$. Thus $\overline{b}_0 = \overline{c}_0 = 0$, and so $p^2 \mid b_0c_0 = a_0$ which is a contradiction, hence at least one of $g$ or $h$ must be constant. \hfill $\Box$

**Corollary 7.** If $f(x) \in \mathbb{Z}[x]$ satisfies Eisenstein’s Criterion then $f(x)$ is irreducible.

**Application:** (Due to Gauss) The cyclotomic polynomial, $x^{p-1} + x^{p-2} + \cdots + 1$, is irreducible.

**Proof.** We have that $x^{p-1} + x^{p-2} + \cdots + 1 = \frac{x^p - 1}{x - 1}$. Let $y = x - 1$, so $\frac{x^p - 1}{x - 1} = \frac{(y+1)^p - 1}{y} = y^{p-1} + \sum_{i=1}^{p-1} \binom{p}{i} y^{i-1} = g(y)$.

This is monic, so (1) is satisfied. Also $p \mid a_i$ for any $i = 1, \ldots, p-1$, and the constant term is just $p$ so it is not divisible by $p^2$. Therefore it satisfied Eisenstein’s Criterion, and $g(y)$ is irreducible over $\mathbb{Z}$, and $\mathbb{Q}$ by Gauss (theorem 13). Now assume that $f(x) = a(x)b(x) \Rightarrow g(y) = f(x-1) = a(x-1)b(x-1) = a(y)b(y)$ which is a contradiction, hence $f$ is not reducible. \hfill $\Box$

**Theorem 18.** (Mason-Strothers or the ABC conjecture for polynomials) Let $a(t), b(t), c(t) \in k[t]$ where $k$ is algebraically closed, $a + b = c$ and they are relatively coprime. Then $\max(\deg\{a, b, c\}) \leq n_0(abc) - 1$ where, for any polynomial $f$, $n_0(f)$ is the number of distinct roots of $f$.

We can use this to prove Fermat’s Last Theorem for polynomials:

**Theorem 19.** (Fermat’s Last Theorem) For $n \geq 3$ there are no nonconstant relatively coprime polynomials $x(t), y(t), z(t)$ such that

$$x(t)^n + y(t)^n = z(t)^n$$

**Proof.** Let $a(t) = x(t)^n$, $b(t) = y(t)^n$, and $c(t) = z(t)^n$. Then $\deg(a) = n\deg(x) \leq n_0(abc) - 1$ by Mason-Strothers, and applying this to $b$ and $c$ as well we find that

\begin{align*}
    n \deg(x) + n \deg(y) + n \deg(z) &\leq 3(n_0(abc) - 1) = 3(n_0(xyz) - 1) \\
    n(\deg(x) + \deg(y) + \deg(z)) &\leq 3(\deg(x) + \deg(y) + \deg(z)) - 3 \\
    (n - 3)(\deg(x) + \deg(y) + \deg(z)) &\leq -3
\end{align*}

but when $n \geq 3$ this left side is nonnegative, and so this is a contradiction. \hfill $\Box$

Now we prove Mason-Strothers:

**Proof.** Let $f = \frac{a(t)}{c(t)}$ and $g = \frac{b(t)}{c(t)}$ which are therefore rational functions in $k(t)$. Then since $a + b = c$, we have that $f + g = 1$ and therefore $f' + g' = 0$. Writing $\frac{f'}{f} + \frac{g'g}{f^2} = 0$ we find that $\frac{b}{a} = \frac{c}{g} = \frac{-f'/f}{g'/g}$. Now decompose $a, b, c$ (which is possible since $k[t]$ is algebraically closed) as

$$a(t) = c_1 \prod (t - \alpha_i)^{m_i} \quad b(t) = c_2 \prod (t - \alpha_i)^{n_i} \quad c(t) = c_3 \prod (t - \gamma_i)^{k_i}$$

Then $f = \frac{a}{c} = \frac{c_1}{c_3} \prod (t - \alpha_i)^{m_i} \prod (t - \gamma_i)^{-k_i}$ and differentiating log $f$, we find that

$$\frac{f'}{f} = \sum \frac{m_i}{t - \alpha_i} + \sum \frac{-k_i}{t - \gamma_i}.$$
Similarly

$$g' = \sum \frac{n_i}{t-\beta_i} + \sum \frac{-k_i}{t-\gamma_i}.$$  

Now let $N_0$ be the common denominator of $\frac{f}{g}$ and $\frac{g'}{g}$, then $N_0 = \prod(t-\alpha_i) \prod(t-\beta_i) \prod(t-\gamma_i)$ (the product is taken over distinct roots) and therefore $\deg N_0 = n_0(abc)$. Now $\deg(N_0\frac{f}{g}) \leq n_0(abc) - 1$. Finally we will use that $\frac{b}{a} = \frac{g'}{g} - \frac{f}{g}$ so we have that $b(N_0\frac{f}{g}) = -a(N_0\frac{f'}{g})$. Since $b$ and $a$ are coprime, $b \mid N_0\frac{f'}{g}$ and therefore $\deg(b) \leq n_0(abc) - 1$. Similarly, $\deg(a) \leq n_0(abc) - 1$. Since $c = a + b$, $\deg(c) \leq n_0(abc) - 1$. 

There is an “elementary” proof of this by Noah Snyder (which is also the one in Lang’s Undergraduate Algebra text), but I actually find this one to be just as elementary and personally preferable (it is the one hinted at in Lang’s graduate Algebra text).

**Application to Calculus** Suppose $F(x,y) \in \mathbb{C}[x,y]$ is irreducible, and consider $\{(x,y) : F(x,y) = 0\} \subseteq \mathbb{C}^2$ (this is known as an algebraic plane curve, for example $x^n + y^n = 1$). The multivalued function $y(x)$ is called an algebraic function, and we now consider the algebraic integral in the Main Theorem of Integral Calculus.

**Theorem 20.** (Main Theorem of Integral Calculus) Let $g(x,y) \in \mathbb{C}(x,y)$ be any rational function, and consider $\int g(x,y)dx$ where $y = f(x)$. Then TFAE:

1. $\int g(x,y)dx$ is an elementary function for any $g$
2. There exist nonconstant rational functions $x(t), y(t) \in \mathbb{C}(t)$ such that $F(x(t), y(t)) = 0$.

Example:

1. Fermat’s Theorem: $x^n + y^n = 1$ for any $n \geq 3$ has no solution in the rational functions because not all integrals of the form $\int g(x, \sqrt[2]{1-x^n})dx$ are elementary (computable).
2. Consider a circle, $x^2 + y^2 = 1$. Note that

$$\left(\frac{t^2-1}{t^2+1}\right)^2 + \left(\frac{2t}{t^2+1}\right)^2 = 1$$

and therefore all integrals of the form $\int g(x, \sqrt{1-x^2})dx$ are computable. This is called Euler’s rationalizing substitution. To perform the integration, use a change of variables to convert it into a rational function, and then use partial fractions.

### 10 Modules

Modules can be thought of as a way to perform Linear Algebra over a ring $R$.

**Warning:** In Linear Algebra abstract vector spaces are isomorphic to $\mathbb{R}^n$. In Algebra, free $R$-modules are similar to $\mathbb{R}^n$, but $R$-modules in general are not.

Let $R$ be any ring with identity, not necessarily commutative.

**Definition 1.** A left $R$-module $M$ is a set with two operations:

1. Addition within the module: $M \times M \to M$, $(m, n) \mapsto m + n$
2. Scalar multiplication by $R$: $R \times M \to M$, $(r, m) \mapsto rm$

which satisfies the following axioms:

1. $(M, +)$ is an Abelian group.
2. Scalar multiplication is distributive:

\[(r + r')m = rm + r'm \quad r(m + m') = rm + rm'\]

3. Scalar multiplication is an action:

\[(rs)m = r(sm) \quad 1 \cdot m = m\]

Modules are Abelian groups with an extra structure, action by $R$. Constructions with modules come from constructions of Abelian groups, so make sure the action is understood. If $R$ is commutative, “module” is equivalent to “left-module”.

Examples:

- If $R = k$ is a field, then $k$-modules are the same as $k$-vector spaces.
- If $R = \mathbb{Z}$, the $\mathbb{Z}$-modules are just Abelian groups. Take any Abelian group $A$, then for any $n \in \mathbb{Z}_{>0}$ and $a \in A$ we have that
  \[n \cdot a = \left(1 + \cdots + 1\right) \cdot a\]
  \[= 1 \cdot a + \cdots + 1 \cdot a\]
  \[= a + \cdots + a.\]

  Similar restrictions (due to distributivity and the fact that it is an action) force our definition of what scalar multiplication can be to agree with the normal group structure on $A$.

- $R$ is, itself, an $R$-module, where scalar multiplication is just the normal multiplication on $R$, and the axioms of being an action and distributivity follow from the axioms for a ring.

- $R^n = R \times \cdots \times R$ is a free $R$-module of rank $n$, where addition and scalar multiplication is defined component-wise.

- $\mathbb{Z}_2$ is an example of a $\mathbb{Z}$-module which is not a free $\mathbb{Z}$-module.

**Definition.** We say that an $R$-module $M$ has torsion if there exists a nonzero $m \in M$ and a nonzero $r \in R$ such that $rm = 0$. (Essentially there are zero divisors.) If no such $m$ and $r$ exist then $M$ is torsion-free.

Examples:

- $\mathbb{Z}_2$ has torsion: take $2 \in \mathbb{Z}$ and $1 \in \mathbb{Z}_2$.

- $\mathbb{Q}$ is an example of a torsion-free but not free $\mathbb{Z}$-module. The reason is that $\mathbb{Q}$ is divisible: for all $n \in \mathbb{Z}, q \in \mathbb{Q}$ there exists $q' \in \mathbb{Z}$ such that $nq' = q$. But a free $\mathbb{Z}$-module is not divisible: Take $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ where the 1 is in the $i$-th place.

Typically, an Abelian group can be made into an $R$-module in many different ways, for various $Rs$. $\mathbb{Z}_2$ is a $\mathbb{Z}$-module (not free), it is a $\mathbb{Z}/2\mathbb{Z}$ module (free), it is a $\mathbb{Z}/4\mathbb{Z}$ module as well. $\mathbb{C}$ is a $\mathbb{Z}$-module, as well as a $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$-module.

Noncommutative Example: Let $R = \text{Mat}_n(k)$, and let $M = k^n$. Defining the standard matrix multiplication from $R \times M \to M$, we see that $M$ is a left $R$-module.
10.1 Submodules

**Definition.** Consider an $R$-module $M$. We say that $N \subseteq M$ is an $R$-submodule if

1. $N$ is a subgroup of $M$
2. $N$ is closed under action by $R$, i.e. $\forall r \in R, n \in N$, $rn \in N$.

Note that
- A $k$-submodule is a vector subspace
- A $\mathbb{Z}$-submodule is a subgroup
- An $R$-submodule of $R$ is a (left) ideal

10.2 Algebras

**Definition.** Let $R$ be a commutative ring with identity. An $R$-algebra is a ring $A$ with a homomorphism $\varphi : R \to A$ such that $\varphi(1_R) = 1_A$ and $\varphi(R) \subseteq Z(A)$ (i.e. $\varphi(R)$ must commute with every element of $A$).

Note that $A$ is also an $R$-module if we define $r \cdot a = \varphi(r)a$. The image of $R$ must commute with $A$ because we want $\text{Hom}_R(M, N)$ to be an $R$-module, see section ??.

Examples:
- $k[x]$ is a $k$-algebra.
- $\text{Mat}_n(k)$ is a $k$-algebra.
- Any ring is a $\mathbb{Z}$-algebra. $n \mapsto 1_R + \cdots + 1_R$ $n$ times

10.3 Module Homomorphisms

**Definition.** Let $M, N$ be $R$-modules. A module homomorphism is a function $\varphi : M \to N$ such that

1. $\varphi$ is a homomorphism of Abelian groups (i.e. $\varphi$ is additive)
2. $\varphi(rm) = r\varphi(m)$ for $r \in R, m \in M$

In other words, $\varphi$ is $R$-linear.

Homomorphisms of $k$-modules are the same as linear transformations.

Example: $\varphi : \mathbb{C} \to \mathbb{C}$ where $\varphi(z) = \overline{z}$. Is this a homomorphism of $\mathbb{C}$-modules? No, since $\varphi(wz) \neq w\varphi(z) = w\overline{z}$. It is a homomorphism of $\mathbb{R}$-modules though. We could turn it into a homomorphism of $\mathbb{C}$-modules by defining the action of $\mathbb{C}$ in the second module to be the twisted action, i.e. $w \cdot z = \overline{w}z$.

**Definition.** Two $R$-modules $M$ and $N$ are isomorphic if there is a bijective homomorphism $\varphi : M \to N$.

Example: $(2) \subseteq \mathbb{Z}$, $(2) \cong \mathbb{Z}$ as a $\mathbb{Z}$-module by the homomorphism $\varphi : \mathbb{Z} \to (2)$ which maps $k \mapsto 2k$.

More generally, if $R$ is a domain and $(x) \subseteq R$ is a left principal ideal then $(x)$ is isomorphic to $R$ as an $R$ module via the homomorphism mapping $r \mapsto rx$ (which is injective since $R$ is a domain). This can be taken to be the definition of a PID: Principal Ideal Domains are domains $R$ such that every submodule of $R$ is isomorphic to $R$.

10.4 Hom

**Definition.** Let $M, N$ be $R$-modules. Then $\text{Hom}_R(M, N)$ is the set of homomorphisms from $M$ to $N$.

Note that
1. $\text{Hom}_R(M, N)$ is an Abelian group.
2. If $R$ is commutative then $\text{Hom}_R(M, N)$ is also an $R$-module.