Math 210B lecture notes

Nakul Khambhati

February 25, 2023

Contents

Part I

Rings

1 Introducting to rings

1.1 Definitions

Definition 1.1.1. A ring is a set R with two binary operations $x + y$, xy such that:

(R1) (R,+) is an abelian group

(R2) $(xy)z = x(yz)$

(R3) $\exists 1 \in R : x1 = x = 1x$

(R4) $(x + y)z = xz + yz$ and $z(x + y) = zx + zy$

If (R5) $\forall x, y \in R : xy = yx$ holds then R is called a commutative ring.

Proposition 1.1.1. $0x = x0 = 0$

Proof. $0x = (0 + 0)x = 0x + 0x$ so $0x = 0$. □

Proposition 1.1.2. $(-x)y = x(-y) = -(xy)$

Proof. $xy + (-x)y = (x - x)y = 0y = 0$ so $(-x)y = -(xy)$ □

Example 1.1.1. $R = \{0\}$ is called the zero ring. Then $1 = 0$. Conversely, if $1 = 0$ then for any $x \in R, x = 1x = 0x = 0$. By contraposition, if $R \neq \{0\}$, then $1 \neq 0$

Definition 1.1.2. We say that $x \in R$ is *invertible* if $\exists y \in R : xy = yx = 1$ and we write $y = x^{-1}$. It also follows that $y^{-1} = x$.

The set of invertible elements of R form a group $R^\times = \{x \in R : x \text{ is invertible}\}$.

Definition 1.1.3. We say R is a division ring if $R^\times = R \setminus \{0\}$. A field is a commutative division ring.

Let R be a commutative ring, $x \in R$ is a zero divisor if $\exists y \in R, y \neq 0$ such that $xy = 0$.

Definition 1.1.4. R is a domain R is a non-zero commutative ring having no non-zero zero divisors i.e. $xy = 0 \implies x = 0 \vee y = 0$.

Proposition 1.1.3. *Fields are domains.*

Proof. Let R be a field, $x, y \in R$ such that $xy = 0$. We want to show one of them must be 0. Let $x \neq 0$. $\therefore \exists x^{-1}$ such that $x^{-1}xy = 0$ which implies $y = 0$. Thus it is a domain. □

Example 1.1.2.

1. $\mathbb{Z}, \mathbb{Z}^\times = \{\pm 1\}$ so it's not a field, but it is an integral domain
2. $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ are fields
3. Let R be a ring, $M_n(R) = \{n \times n \text{ matrices over } R\}$. $M_n(R) = GL_n(R)$
4. $\mathbb{Z}/n\mathbb{Z}, (\mathbb{Z}/n\mathbb{Z})^\times = \{[a] : \gcd(a, n) = 1\}]$. When n is a prime, $\phi(n) = n - 1$ and $R^\times = R \setminus \{0\}$ so it is a field.

   $\mathbb{Z}/n\mathbb{Z}$ is a field $\iff$ n is a prime $\iff$ $\mathbb{Z}/n\mathbb{Z}$ is a domain.
5. Let $(A, +)$ be an abelian group. Set $R = \text{End}(A) = \text{Hom}(A, A)$. Then R is a ring by addition and composition of functions.
6. Let $\mathbb{H}$ be a vector space over $\mathbb{R}$ with basis $\{1, i, j, k\}$. We wish to make this a ring. By distributivity, it suffices to specify multiplication rules for the basis elements.

	i	**j**	**k**
i	-1	k	j
j	-k	-1	i
k	j	-i	-1

   This is a division ring although it is clearly not commutative. We can prove this by introducing the norm $N(a1+bi+cj+dk) = a^2+b^2+c^2+d^2$. It can be checked that $N(z_1z_2) = N(z_1)N(z_2)$. Also, define $\overline{z} = a1-bi-cj-dk$. Then, $z\overline{z} = N(z)1$. So, for $z \neq 0, z^{-1} = \dfrac{\overline{z}}{N(z)}$. However, $\mathbb{H}_\mathbb{C} \cong M_2(\mathbb{C})$ so it's not a division ring.
7. Let R be a ring, define $R[x] = \{a_0+a_1x+\cdots+a_nx^n\}$. If R is commutative (domain), then $R[x]$ is commutative (domain).

   By induction, define $R[x_1, \cdots, x_n] = R[x_1, \cdots, x_{n-1}][x_n]$ all x_i commute so that we can arrange terms as monomials $x_1^{k_1} \cdots x_n^{k_n}, k_i \geq 0$.

   For any (infinite) set X of variables, we can define $R[X] = \bigcup_{Y \subset X} R[Y]$ where Y is finite. We also have $R\langle X \rangle = \{\text{set of R-linear combinations of monomials}\}$ where a monomial is a *word* in X.

1.2 Ring homomorphisms

Definition 1.2.1. Let R, S be rings. A ring homomorphism is a map $f : R \to S$ that preserves operations

1. $f(x+y) = f(x) + f(y)$
2. $f(xy) = f(x)f(y)$
3. $f(1) = 1$

Remark. Interestingly, $\mathrm{Hom}_{\mathrm{Rings}}(R, S)$ can be empty. For example, there is no ring homomorphism from $\mathbb{Q}$ to $\mathbb{Z}$.

1.3 Category of rings

The category Rings has objects rings and arrows ring homomorphisms. $\mathbb{Z}$ is an initial object and 0 is a final object.

Example 1.3.1. Let X be a set and consider $\mathbb{Z}\langle X\rangle$. We want to describe ring homomorphisms of the form $f : \mathbb{Z}\langle X\rangle \to R$ where R is some ring. It suffices to give the image for each $x \in X$. In other words, this data is the same as a map $f : X \to R$. So, we have $\mathrm{Hom}(\mathbb{Z}\langle X\rangle, R) \cong \mathrm{Maps}(X, R)$. This tells us that the construction $F : X \to \mathbb{Z}\langle X\rangle$ is a functor and it is left-adjoint to the forget functor for rings.

Example 1.3.2 (Group ring)**.** Let R be a ring, G be a group.

$R[G] := \left\{ \sum_{g\in G} r_g g,\ r_g \in R \right\}$ and we define multiplication as $(rg)(r'g') := (rr')(gg')$.

Clearly $G \subset R[G]^\times$ via $g \mapsto 1g$. It remains an open question whether for $R = \mathbb{Z}$, $G = \mathbb{Z}[G]$.

Let S be a ring, and $f : \mathbb{Z}[G] \to S$ be a ring homomorphism. Then $f(G) \subset S^\times$ and we can restrict it to $f|_G : G \to S^X$ a group homomorphism. Conversely, if we are given some $h : G \to S^\times$ a group homomorphism. We can construct $f : \mathbb{Z}[G] \to S$ via the formula $f(\sum r_g g) := \sum r_g h(g)$.

Therefore, we have $\mathrm{Hom}_{Rings}(\mathbb{Z}(G), S) \cong \mathrm{Hom}_{Groups}(G, S^\times)$ and we have an adjunction of functors.

1.4 Subrings

Let S be a ring, $R \subset S$ a subset. For it to be a subring, we need to check:

1. $x, y \in R \implies x + y \in R \wedge xy \in R$
2. $1_S \in R$
3. $x \in R \implies -x \in R (\because 0 \in R)$
4. And we additionally impose that $1_R = 1_S$

Example 1.4.1.
1. $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$
2. If $f : R \to S$ is a ring homomorphism, then $\mathrm{Im}(f) \subset S$ subring.

2 Ideals

2.1 Definitions

Definition 2.1.1. Let R be a ring, $I \subset R$ be a subset. I is a left-ideal of R if:

1. I is a subgroup of $(R, +)$
2. $\forall x \in R : xI \subset I$

I is an ideal if it's both a left and right ideal.

Example 2.1.1.

1. $0 \subset R$ zero ideal, $R \subset R$ unit ideal
2. Let $(I_k)_{k \in K}$ be a family of (left) ideals. Then, $\bigcap_{k \in K} I_k$ is a (left) ideal.
3. Let $X \subset R$ subset. The smallest (left) ideal containing X is called the (left) ideal generated by X, $\langle X \rangle$.

   $\langle X \rangle = \bigcap_{X \subset I} I = \{\sum_X r_x x, r_x \in R\}$

   It can be checked that the set described is an ideal and must be contained in any other ideal containing X.

   If $X = \{x\}, \langle x \rangle = \{rx, r \in R\} = Rx$ principal left ideal of x.
4. If $I \subset R$ is a (left) ideal such that it contains an invertibe element i.e. $I \cap R^\times = \emptyset$ then $I = R$.

   Proof. If $x \in I, x \in R^\times$, $x^{-1}x = 1 \in I$ so $R1 \subset I$ and $I = R$. □
5. Let $(I_k)_{k \in K}$ be a family of (left) ideal of R. We want the smallest ideal containing them. A union may not be an ideal.

   $\langle \bigcup I_k \rangle = \sum_{k \in K} I_k = \left\{ \sum_{k \in K} x_k, x_k \in I_k \right\}$

2.2 Factor rings

Let $I \subset R$ be a 2-sided ideal.

Consider the factor *group* $R/I = \{r + I, r \in R\}$. We wish to give this the structure of a ring.

Define multiplication as $(x + I)(y + I) := xy + I$.

Proposition 2.2.1. *The above is well-defined.*

Proof. Let $x + I = x' + I$ and $y + I = y' + I$. So $x' - x \in I$ and $y - y' \in I$. We wish to show that $x'y' - xy \in I$. $x'y' - xy = (x'y' - x'y) + (x'y - xy) = x'(y' - y) + (x' - x)y \in I$. □

Proposition 2.2.2. *R/I is a factor ring with $1_{R/I} = 1 + R$, $0_{R/I} = 0 + I = I$.*

Proof. The proof is trivial since the canonical group homomorphism $\pi : R \to R/I$ that sends $r \mapsto r+I$ is easily shown to be a ring homomorphism as well. □

Proposition 2.2.3. *Let $f : R \to S$ be a ring homomorphism, $I = \mathrm{Ker}(f) \subset R$ is an ideal.*

Proof. Let $x \in I, y \in R$. $f(x) = 0$ so $f(yx) = f(y)0 = 0$ so $yx \in I$. □

Remark. Note that we observe get the correspondences subgroups $\iff$ left/right ideals and normal subgroups $\iff$ two-sided ideals.

Theorem 2.1 (first isomorphism)**.** *Let $f : R \to S$ be a ring homomorphism. Then $R/\operatorname{Ker} f \cong Im(f)$ as rings.*

Proof. Omitted. □

Example 2.2.1.

1. $\mathbb{Z}/n\mathbb{Z}$ the factor ring
2. $\mathbb{R}[X]/\langle X^2 + 1\rangle \cong \mathbb{C}$

   Consider $f : \mathbb{R}[X] \to \mathbb{C}$ where $p(x) \mapsto p(i)$. It is clearly surjective as $a + bx \mapsto a + bi$ and it can be shown that $\mathrm{Ker}(f) = \langle X^2 + 1\rangle$. The rest follows from first isomorphism.
3. $R \times S = \{(r, s), r \in R, s \in S\}$ external product of rings, where we define operations component wise. $1_{R\times S} = (1_R, 1_S)$. We can also take arbitrary products of a family $\prod_{i\in I} R_i$.

2.3 Internal product

Let $S = R_1 \times \cdots \times R_n$. Define $e_i = (0, \ldots, 1, \ldots, 0)$ where the 1 is in the ith position. The collection $\{e_i : i \in \{1, \ldots, n\}\}$ has the following properties:

1. $e_i^2 = e_i$ (idempotents)
2. $e_i e_j = 0$ if $i \neq j$ (orthogonal)
3. $\sum_{i=1}^{n} = 1_S$ (partition of 1_S)
4. $\forall x \in S : e_i x = x e_i$ (central)

In summary, we have a partition of 1_S into central orthogonal idempotents.

Conversely, let R be a ring with $e_1, \ldots, e_n \in R$ such that $(1)-(4)$ above holds. We define $R_i = Re_i = \{xe_i, x \in R\} \subset R$. It is clearly closed under addition. Also, let $x, y \in R$ such that $xe_i, ye_i \in R$. Then $xe_iye_i = xye_i^2$ by centrality, which equals xye_i by idempotents. In fact, it is a ring with $1_{R_i} = e_i$. However, note that it is not a subring since $1_{R_i} \neq 1_R$ if the partition is non-trivial.

Consider $f : R_1 \times \cdots \times R_n \to R$ that maps $(r_1, \ldots, r_n) \mapsto r_1 + \cdots + r_n$.It is easily seen to be a group homomorphism.

Proposition 2.3.1. *The above map f is in fact a ring isomorphism.*

Proof. First we show that f is a ring homomorphism.
$f((r_1, \ldots, r_n)(r'_1, \ldots, r'_n)) = f(r_1r'_1, \ldots, r_nr'_n) = \sum_I r_ir'_i$
$f(r_1, \ldots, r_n)f(r'_1, \ldots, r'_n) = (r_1 + \cdots + r_n)(r'_1 + \cdots + r'_n) = \sum_{i,j} r_ir'_j = \sum_I r_ir'_i$
$f(1) = \sum_I e_i = 1_R$ since the e_i partition unity.

Now we show that the map is surjective and injective. Let $r \in R$. Then, $f(re_i, \ldots, re_n) = r(e_1 + \cdots + e_n) = r$. Let $(r_1, \ldots, r_n) \in ker(f)$ i.e. $\sum_I r_i = 0$. Recall that each $r_i = x_ie_i$ for some $x_i \in R$. So $\sum_I x_ie_i = 0$. Multiplying both sides by e_j yields $x_j = 0 \; \forall j \in I$. So, each $r_j = x_je_j = 0$. □

Example 2.3.1. Let R be a ring and consider the ring $D_n(R) \subset M_n(R)$ of diagonal matrices. It can be checked that $e_i = D_i$, where D_i is defined as the matrix where all entires are 0 except 1 in the (i,i)-th entry, is a set of idempotents satisfying the above. Also, $R_i = D_n(R)e_i \cong R$. Therefore, $D_n(R) \cong R \times \cdots \times R$ where the isomorphism is clear.

2.4 Relatively prime ideals

Let $I \subset R$ be an ideal. For $x, y \in R$, we say that $x \equiv y \pmod{I}$ if $y - x \in I$.

Definition 2.4.1. Let $I, J \in R$ be ideals. We say that they are co-prime if $I + J = R$.

Example 2.4.1. $n\mathbb{Z}, m\mathbb{Z}$ are coprime $\iff \gcd(n, m) = 1$.

Theorem 2.2 (chinese remainder theorem)**.** *Let R be a ring, $I_1, \ldots, I_n$ pairwise co-prime. Let $a_1, \ldots, a_n \in R$. Then $\exists a \in R$ such that $a \equiv a_i \pmod{I}$ for all i.*

Proof. We proceed by induction. The case for $n = 1$ is trivial so we begin with $n = 2$. Let $I_1 + I_2 = R$. We are given $a_1, a_2 \in R$. Then, $a_1 - a_2 \in R$ so we can write it as $x_1 + x_2$ for $x_1 \in I_1, x_2 \in I_2$. Then, $a_1 - a_2 = x_1 + x_2 \Rightarrow a_1 - x_1 = a_2 + x_2$. This gives us the desired a. Now, assume $n - 1$ and prove n. First, we prove a lemma.

Lemma 2.3. *The ideals $I_1 \cap \cdots \cap I_{n-1}$ and I_n are co-prime.*

Proof of lemma. Note that it suffices to show $\exists x \in \bigcap I_i, \exists y \in I_n$ such that $x + y = 1$. We know that $I_i + I_n = R$ for $1 \leq i \leq n-1$. So, $\exists x_i \in I_i, y_i \in I_n$ such that $x_i + y_i = 1$. Then, $1 = (x_1 + y_1) \cdots (x_n + y_n) = x_1 \cdots x_n + (\text{monomials in y}) \in I_1 \cap \cdots \cap I_{n-1} + I_n = R$. □

We can now continue with the proof. From $n-1$, we get that $\exists b \in R$ such that $b \equiv a_i \pmod{I_i}$ for $1 \leq i \leq n-1$. Now, from the $n = 2$ case and the above lemma, we know that $\exists a \in R$ such that $a \equiv b \bmod(I_1 \cap \cdots \cap I_{n-1})$ and $a \equiv a_n \pmod{I_n}$. □

Corollary 2.3.1. $R/(\bigcap I_i) \cong (R/I_1) \times \cdots \times (R/I_n)$

Proof. Let $f : R \to (R/I_1) \times \cdots \times (R/I_n)$ be the component-wise canonical projection. It is surjective by the Chinese Remainder Theorem and has kernel $\bigcap I_i$. The result follows from First Isomorphism. □

Example 2.4.2. Let $m_1, \ldots m_n \in \mathbb{Z}$ be relatively prime. Then apply the theorem to $R = \mathbb{Z}, I_i = \mathbb{Z}/m_i\mathbb{Z}$. Then $\mathbb{Z}/m_1 \cdots m_n\mathbb{Z} \cong (\mathbb{Z}/m_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_n\mathbb{Z})$. A similar result follows for the prime factorization of any integer $N = p_1^{k_1} \cdots p_n^{k_n}$. It follows that if an integer N has n distinct prime factors, then $\mathbb{Z}/N\mathbb{Z}$ has 2^n idempotents.

Proposition 2.4.1. *If $e \in R$ is a central idempotent, then so is $f = 1 - e$. Moreover, e, f are orthogonal and partition unity.*

Proof. $f^2 = (1-e)^2 = 1 - 2e + e^2 = 1 - 2e + e = 1 - e = f$.
$ef = e(1-e) = e - e^2 = e - e = 0$.
They sum to 1 by definition. □

2.5 Prime and maximal ideals

For this section, we let R denote a *commutative* ring.

Definition 2.5.1. An ideal $P \subset R$ is prime if $xy \in P \implies x \in P \vee y \in P$.

Proposition 2.5.1. *An ideal $P \subset R$ is prime $\iff$ R/P is a domain.*

Proof. Let $xy \in P$ i.e. $\overline{xy} = \overline{0}$ in R/P. Then $x \in P \vee y \in P \iff \overline{x} = \overline{0} \vee \overline{y} = \overline{0} \in P/R$. □

Example 2.5.1.

1. $n \geq 0, n\mathbb{Z}$ is prime $\iff$ n is prime or $n = 0$
2. 0 is prime $\iff$ R is a domain.

We want to show that every non-zero ring has a prime ideal. This is not very easy to do. For this, we will first introduce the concept of a maximal ring.

Definition 2.5.2. An ideal $M \subset R$ is maximal if $M \subset I \subset R \Rightarrow I = M \vee I = R$.

Lemma 2.4. *A ring R is a field $\iff$ R has exactly two ideals.*

Proof. In a field, if $I \neq 0$ then $\exists a \in I, a \neq 0$. So, $a^{-1}a = 1 \in I \Rightarrow I = R$. On the other hand, if a ring has exactly two ideals, every non-zero element is invertible so it's a field. □

Corollary 2.4.1. *An ideal M is maximal $\iff$ R/M is a field by the above lemma and the correspondence theorem.*

Corollary 2.4.2. *A maximal ideal M is prime since every field is a domain. The converse is not true.*

Example 2.5.2.
1. $n \geq 0, n\mathbb{Z}$ is max $\iff$ n is prime
2. 0 max in $R \iff R$ is a field

Definition 2.5.3. Let X be a partially-ordered set (poset), $x \leq y$ is a transitive relation that exists between some (but not necessarily all) elements in X. $C \subset X$ is a chain if $\forall x, y \in C$ we have $x \leq y \vee y \leq x$. Let $Y \subset X$ be a subset. An upper bound for Y is an element $x \in X$ such that $y \leq x \; \forall y \in Y$. Also, x is a maximal element if $x' \leq x$ then $x' = x$.

Lemma 2.5 (Zorn)**.** *Let X be a nonempty poset such that every chain has an upper bound (in X). Then X has a maximal element. This is equivalent to the Axiom of Choice.*

Theorem 2.6. *Every nonzero commutative ring R has a maximal ideal. Therefore, it has a prime ideal.*

Proof. Let $X = \{\text{set of ideals } I \subset R, I \neq R\}$ be a poset ordered by inclusion. It is clearly nonempty since $0 \in X$. Let $C \in X$ be a chain. We claim that $J = \bigcup_{I \in C} I$ is an ideal. For arbitrary unions, $0 \in J$ and $y \in J, x \in R \Rightarrow xy \in J$. Here, the poset allows us to prove $x, y \in J \Rightarrow x + y \in J$ since $x \in I_\alpha, y \in I_\beta$ implies one is contained within the other so their sum is contained within the bigger one. Since $1 \notin I$ for any I, $1 \notin J$ so $J \in X$. Also, $I \subset J$ for all I so J is an upper bound for C. Then, by Zorn's lemma, J is a maximal ideal of R. □

3 Principal ideal rings

Definition 3.0.1. A ring R is a principal ideal ring if every ideal $I \subset R$ is principal.

Example 3.0.1.
1. $\mathbb{Z}$ is a PIR. Every ideal of $\mathbb{Z}$ must be a subgroup so it's of the form $n\mathbb{Z} = (n)$.
2. F has $(0), (1)$ as ideals so it is a PIR.

To exhibit that certain rings are PIR's, we introduce the class of Euclidean rings.

3.1 Euclidean rings

Definition 3.1.1. A ring R is Euclidean if $\exists \phi : R \setminus \{0\} \to \mathbb{Z}_{n \geq 0}$ such that division is possible. More formally, such that $\forall a, b \in R \; b \neq 0 \; \exists q, r \in R$ such that $a = bq + r$ where $r = 0$ or $\phi(r) < \phi(b)$.

Theorem 3.1. *Let R be a ring. R is Euclidean $\Rightarrow$ R is a PIR.*

Proof. Let R be a Euclidean ring. Let $I \subset R$ be an ideal. Pick an element $b \in I, b \neq 0$ such that $\phi(b)$ is minimal. We now show that $I = (b)$. Let $x \in I$. Since b is non-zero, we can write $x = qb + r$ for $q, r \in R$. It suffices to show that $r = 0$. Assume not, then $\phi(r) < \phi(b)$. But since $r = x - qb \in I$, this contradicts the minimality of $\phi(b)$ in I. Therefore, $r = 0$. □

Example 3.1.1.

1. $\mathbb{Z}$ is euclidean with $\phi(x) = |x|$.
2. Let F be a field, $R = F[x]$ a polynomial ring. This is a Euclidean ring with $\phi(f) = deg(f)$. Note that F must be a field. For example, in $\mathbb{Z}[x]$ we cannot divide $x + 1$ by $2x$.
3. $\mathbb{Z}[i] = \{a + bi, \; a, b \in \mathbb{Z}\}$ is euclidean via $\phi(a + bi) = a^2 + b^2$. We can compute division with the help of the absolute value function. However, this might have coefficients in $\mathbb{Q}$. However, one can get around this difficulty by observing that we can always find integers *close enough* to these rational coefficients such that the division algorithm doesn't break.

Proposition 3.1.1. *The above ϕ makes $\mathbb{Z}[i]$ a Euclidean ring.*

Proof. Ommited. □

4 Factorization in commutative rings

4.1 Definitions

Definition 4.1.1. Let R be a commutative ring. Let $a, b \in R, b \neq 0$. We say that b divides a, denoted $b|a$, if $\exists c \in R : a = bc$. Equivalently, $bR \neq 0$ and $aR \subset bR$.

Definition 4.1.2. Let $a, b \in R$. We say that a and b are associates, denoted $a \sim b$, if $b|a$ and $a|b$. Equivalently, $aR = bR \neq 0$.

Now suppose that R is a domain.

Proposition 4.1.1. $a \sim b \iff \exists u \in R^\times : b = au$

Proof. If $a \sim b$ then $\exists c : a = bc$ and $\exists d : b = ad$. Therefore, $a = adc \Rightarrow 1 = dc \Rightarrow d, c \in R^\times$. So, a and b are one invertible element apart. The converse is clear. □

4.2 Primes and irreducibles

Definition 4.2.1. An element $c \in R$ is irreducible if $c \neq 0, c \notin R^\times$ and $c = xy \Rightarrow x \in R^\times \vee y \in R^\times$.

Example 4.2.1. In $\mathbb{Z}$, c is irreducible $\iff$ $|c|$ is prime

Proposition 4.2.1. *An element $c \in R$ is irreducible $\iff$ cR is maximal in principal ideals.*

Proof. $\Rightarrow$ Assume c is irreducible and let $cR \subset bR \neq R$. We need to show that $bR = cR$. We know that $\exists d \in R : c = bd$. But c is irreducible so either $b \in R^\times$ or $d \in R^\times$. But b is not invertible since $bR \neq R$. So d is invertible and $bR = cR$. $\Leftarrow$ Assume that cR is maximal so $cR \subset bR \subset R \Rightarrow cR = bR$ or $bR = R$. Write $c = xy$ so $cR \subset xR$ and $cR \subset yR$. Assume $cR = xR$ implies that y is invertibe and assuming $xR = R$ implies x is invertible. □

Corollary 4.0.1. *If $a \sim b$ and a is irreducible then b is irreducible.*

Proof. Then, $aR = bR$ is maximal in principal ideals so b is irreducible. □

Definition 4.2.2. An element $p \in R$ is prime if $p \neq 0, p \notin R^\times$ and $p|xy \Rightarrow p|x \vee p|y$. This is equivalent to bR is a nonzero prime ideal.

Proposition 4.2.2. *Every prime element $p \in R$ is irreducible.*

Proof. Let p be a prime element. Let $p = xy$. Then $p|xy$ so $p|x$ or $p|y$. If $x = pz$, then $x = xyz \Rightarrow 1 = yz \Rightarrow y \in R^\times$. The other case follows similarly. So, p is irreducible. □

In general, the converse is not true.

Example 4.2.2. Consider $R = \mathbb{Z}[\sqrt{-5}] = \left\{a + b\sqrt{-5}, a, b \in \mathbb{Z}\right\} \subset \mathbb{C}$ a subring. We claim that not all primes are irreducible. For example 2 is irreducible but not prime. $2|6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ but $2 \nmid 1 + \sqrt{-5} \wedge 2 \nmid 1 - \sqrt{-5}$. On the other hand, assume $2 = xy$. So $|2|^2 = |x|^2|y|^2$. By checking integers, either x or y are ± 1 which are invertible. So, 2 is irreducible but not prime.

Proposition 4.2.3. *If R is a PID then every irreducible is prime.*

Proof. Let R be a PID. Let $c \in R$ be an irreducible element i.e. $cR \neq 0$ and cR is maximal in principal ideals. Since R is a PID, cR is just maximal. Therefore, cR is prime $\Rightarrow c$ is prime. □

Corollary 4.0.2. $\mathbb{Z}[\sqrt{-5}]$ *is not a principal ideal domain.*

4.3 Uniqueness of factorization

Definition 4.3.1. R *admits factorization* if every $a \in R, a \neq 0, a \notin R^\times$ can be written as $a = c_1 \cdots c_n \iff aR = (c_1R) \cdots (c_nR)$ where all c_i are irreducible elements in R.

Definition 4.3.2. Factorization in R is *unique* if whenever $c_1 \cdots c_n = d_1 \cdots d_m$ $(c_1R \cdots c_nR = d_1R \cdots d_mR)$ for c_i, d_j irreducible, we have $n = m$ and $\exists$ a permutation $\sigma \in S_n$ such that $c_i \sim d_{\sigma(i)}$ $(c_iR = d_{\sigma(i)}R)$.

Proposition 4.3.1. *Let R be a domain.*

1. *If R admits factorization, then the factorization in R is unique $\Rightarrow$ every irreducible is prime.*
2. *If every irreducible element is prime, then factorization in R is unique.*

Proof. $\Rightarrow$ Let $c \in R$ be irreducible. Assume that $c|xy$ so $xy = cd$. Since factorization is unique, $(xR)(yR) = (cR)(dR)$. By replacing each x, y, d with their factorizations, $(x_1R \cdots x_nR)(y_1R \cdots y_mR) = (cR)(d_1R \cdots d_kR)$. Then, by uniqueness of factorization, we must have $cR = x_iR \vee cR = y_iR$ for some i. If $cR = x_iR$ then $c \sim x_i$ so $c|x$. Otherwise, if $cR = y_jR$ then $c \sim y_j$ so $c|y$. Therefore, c is prime.
$\Leftarrow$ Assume that every reducible in R is prime. Let $a_1R \cdots a_nR = b_1R \cdots b_mR$. We will now proceed via induction on n. Recall that since all a_i, b_i are irreducible, they are also prime. So, $a_n|b_1 \cdots b_m \Rightarrow a_n|b_j$ for some j. We can relabel so that $a_n|b_m$. But since b_m is irreducible, $b_m = ca_m$ for some $c \in R^\times$. Therefore, $a_nR = b_mR$. By induction, this is true for all n and $m = n$. □

4.4 Unique factorization domains

We are now interested in looking at the class of rings that admit factorization and, in particular, that factorization is unique.

Definition 4.4.1. A unique factorization domain (UFD) is a domain in which every element has a unique factorization into irreducibles.

Theorem 4.1. *A domain R is a UFD $\iff$ R admits factorization and every irreducible is prime.*

Proof. Proposition 4.3.1 □

In the above theorem, we have captured the fact that uniqueness of factorization is equivalent to every irreducible being prime. Now, we need a condition for existence of factorization.

Proposition 4.4.1. *Let R be a commutative ring. Then, TFAE:*

1. *Every ideal $I \subset R$ is finitely generated.*
2. *For every infinite chain of ideals $I_1 \subset I_2 \subset \cdots$ there exists some $n : I_n = I_{n+1} = \cdots$. In other words, every infinite chain of ideals stabilizes.*
3. *Every nonempty set of ideals has a maximal element by inclusion.*

Proof. (1) $\Rightarrow$ (2): Assume that every ideal I in R is finitely generated. Consider an infinite chain of ideas $I_1 \subset I_2 \subset \cdots$. Now, consider $\bigcup_{k=1}^{\infty} I_k = I$. Since each I_k is finitely generated, so is I. We can write $I = (x_1, \ldots, x_n)$. Since this is a chain, $\exists I_k : x_1, \ldots, x_m \in I_k$. Therefore, $I \subset I_k$. So, $\forall m \geq k$, $I_k \subset I_m$ and $I_m \subset I \subset I_k$ so $I_m = I_k$.
(2) $\Rightarrow$ (3): Assume that there is some nonempty set A of ideals without a maximal element. Then, pick $I_1 \in A$ not maximal so $\exists I_2 : I_1 \subsetneq I_2$. This process will go on infinite contradicting the fact that every infinite chain stabilizes.
(3) $\Rightarrow$ (1): Let $I \subset R$ be an ideal of R. Consider the set A of finitely generated ideals $\subset I$. Since $0 \in I$ this set is nonempty. Therefore, this set has a maximal element by inclusion. Let $J \in A$ be the maximal element. We claim that $J = I$, then we are done. If this is not the case, we can pick some $x \in I \setminus J$ such that $J \subsetneq J + xR \subset I$. But $J + xR$ is also finitely generated and in I and strictly bigger than J which contradicts the maximality of J. Therefore $I = J$. □

Definition 4.4.2. We call a ring R Noetherian if it satisfies the above.

Proposition 4.4.2. *Every Noetherian domain R admits factorization.*

Proof. Assume that R is a Noetherian domain. Let $A = \{xR : xR \text{ does not admit factorization}\}$ We wish to prove that this set is empty. In search of a contradiction, assume it's not. Then, it has a maximal element by inclusion. Let xR be this maximal element. If it was irreducible, it would not be in this set, so it is reducible into strictly smaller elements. $xR = (yR)(zR)$. We can't have either of yR or xR in A as they are bigger than xR and would contradict the maximality. Therefore, both z and y have factorizations and therefore so does x. Therefore, $A = \emptyset$.

□

Theorem 4.2. *A Notherian domain is a UFD $\iff$ every irreducible element is prime.*

Proof. Theorem 4.1 & Proposition 4.4.2 □

Example 4.4.1. A PID is a UFD. For example, $\mathbb{Z}, \mathbb{Z}[i], F[x]$. In particular, any ring with a Euclidean function admits unique factorization. However, there are UFDs such as $F[x, y]$ that are not PIDs.

Definition 4.4.3. Let R be a UFD. Then, any element xR can be written as $(p_1R)^{k_1} \cdots (p_s sR)^{k_s}$ for each p_i prime. Pick many such x_i. We define $\gcd(x_1, \ldots, x_m) = (p_1R)^{l_1} \cdots (p_nR)^{l_n} = p_1^{l_1} \cdots p_n^{l_n} R$ where each $l_j = \min(k_{1j}, k_{2j}, \ldots, k_{mj})$.

Remark. Let $d = \gcd(x_1, \ldots, x_m)$. Then, $\forall i : d|x_i$. And $(\forall i : y|x_i) \Rightarrow d|y$.

5 Factorization in polynomial rings

Recall that $R \subset R[x_1, \ldots, x_n]$. Also R domain $\Rightarrow R[x]$ domain. Assume R is a domain. Let $f, g \in R[x]$. Then $deg(fg) = deg(f)deg(g)$. We can set $deg(0) = -\infty$. We wish to determine the invertible elements of $R[x]$. Let $fg = 1$. Then $deg(f) + deg(g) = 0$. Therefore, $deg(f) = 0$ and $deg(g) = 0$ so both f, g must be nonzero constants. Also recall that $R \subset S \Rightarrow R[x] \subset S[x]$. If an element is irreducible in $R[x]$ it is obviously irreducible over $S[x]$. However, the converse is not true.

Our goal is to determine irreducibles $f \in R[x]$ when R is a UFD. Clearly, irreducibles in R are also irreducible in $R[x]$ by degree considerations. But must also be elements in $R[x] \setminus R$ that are irreducible.

5.1 Definitions

Definition 5.1.1. Let $f \in R[x]$ be a nonzero polynomial. We define $C(f) =$ gcd(non-zero coefficients) called the content of f.

Example 5.1.1. In $Z[x]$, $C(6x^2 - 14) = 2\mathbb{Z}$.

Definition 5.1.2. A polynomial is called monic if the coefficient of its leading term is 1. Clearly, $C(f) = R$ for f a monic.

Definition 5.1.3. A polynomial f is called primitive if $C(f) = R$.

Example 5.1.2. For $0 \neq a \in R$, $C(f) = aR$. Also, $C(af) = C(a)C(f)$. Finally, for $0 \neq c \in R \subset R[x]$ c is primitive $\iff cR = R \iff c \in R^\times$.

Lemma 5.1 (Gauss)**.** *The product of primitive polynomials f and g is primitive.*

Proof. Let $c \in R$ be an irreducible. Since we are working within a UFD, c is prime. Consider $\pi : R \to R/cR = \overline{R}$. Let $f, g \in R[x]$ primitive. As a result, $\overline{f} \neq 0, \overline{g} \neq 0$. Since (c) is prime, $\overline{R}$ is a domain. As a result $\overline{fg} \neq 0$. Then, there is some coefficient in fg that is not divisible by c. Since c was arbitrary chosen as an irreducible, fg cannot be divided by any c. So, $C(fg) = R$. □

Corollary 5.1.1. *For nonzero $f, g \in R[x]$, $C(fg) = C(f)C(g)$.*

Proof. Let $f, g \in R[x]$. We can always divide by the gcd and get $f = af'$ for f' primitive. So $C(f) = aC(f')$. Similarly, we can write $fg = abf'g'$ and $C(fg) = abC(f'g') = abR$. So $C(fg) = C(f)C(g)$. □

5.2 Fraction fields

Let R be a domain so that $S = R \setminus \{0\}$ is a multiplicative set. Then, from HW, we construct the fraction field $F = S^{-1}R = \left\{ \frac{a}{b}, a, b \in R, b \neq 0 \right\}$. Further, we can imbed $R \subset F, a \mapsto \frac{a}{1}$.

In particular, $R[x] \subset F[x]$. This is useful because $F[x]$ is always a Euclidean ring, which is a PID, which is a UFD.

Lemma 5.2. *Let $f, g \in R[x] \subset F[x]$, then g is primitive. Then, if $g|f$ in $F[x]$, then $g|f$ in $R[x]$. In other words, if g/f exists in $F[x]$ then it has coefficients in $R[x]$.*

Proof. Assume that $f = gh, h \in F[x]$. We want to prove that we can write $h \in R[x]$. Let's eliminate the denominator from this such that for $a \in R : ah \in R[x]$. Then $af = g(ah)$ so $aC(f) = C(g)C(ah) = C(ah)R$ since g is primitive. Let's write $C(ah) = bR$ for some $b \in R$. So $a|b$ and we can write $b = ac$ for $c \in R$. So, $C(ah) = acR$. Then, every coefficient of of ah is divisble by ac. So every coefficient of h is divisble by $c \in R$. Therefore, $h \in R[x]$. □

Proposition 5.2.1. *A nonconstant polynomial $f \in R[x]$ is irreducible $\iff$ f is primitive and irreducible in $F[x]$.*

Proof. $\Rightarrow$ Let $f \in R[x]$ be irreducible in $R[x]$. Therefore, when we pull out the gcd, we get af' for f' primitive but also a must be invertible. So, $C(f) = aR = R$. Therefore, f is also primitive. Now assume $f = gh, g, h \in F[x]$. Our goal is to show that one of them must be an invertible constant. We can multiply by constants to make $g = \frac{b}{a}g'$ for g' primitive in $R[x]$. Therefore, we write $f = (\alpha g')h$. So $g'|f$. Then αh is in $R[x]$ by the previous proposition. Now we have factorized f in $R[x]$ which means that either $g \in F^\times$ or $h \in F^\times$.
$\Leftarrow$ Let $f = gh, g, h \in R[x]$. We want to show that one of them must be an invertibe scalar. Over F this fact is trivial since f irreducible in $F[x]$ so one of g, h is constant. WLOG, assume $g \in R$ is constant. $R = C(f) = g \cdot C(h)$. So we must have $g \in R^\times$. Therefore g is irreducible in $R[x]$. □

Remark. The irreducibles in $R[x]$ are (1) irreducibles in R and (2) $f \in R[x]$ primitive and irreducible over $F[x]$.

Theorem 5.3. *If R is a UFD, then $R[x]$ is a UFD.*

Proof. Assume R is a UFD, we want to show every $R[x]$ admits factorization into irreducibles and each is prime. We can write $f = af'$ for $a \in R$ and f' primitive. Since R is a UFD, we only need a way to factorize primitives. If f' is irreducible in $F[x]$ we are done as it is then irreducible in $R[x]$. So we assume f' is reducible over $F[x]$. Let's right $f' = gh, g, h \in F[x]$. So, by the previous proposition, $f' = gh$ is a factorization over $R[x]$. Then, argue by induction on degree to eventually reach f' is either irreducible or it gets broken down into

constant terms. This is a factorization in $R[x]$.
We now show that this factorization is unique i.e. every irreducible is prime. Let f be irreducible over $R[x]$. Therefore, it is irreducible over $F[x]$ and primitive. Therefore, f is prime over $F[x]$. Since $f|gh \Rightarrow f|g \vee f|h$ in $F[x]$, it carries over to $R[x]$ and we are done. $\square$

Example 5.2.1. Both $F[x_1, \ldots, x_n]$ and $\mathbb{Z}[x_1, \ldots, x_n]$ are UFDs.

At the end of Lec 7 notes: diagram showing classification.

Part II

Modules

6 Introduction to modules

6.1 Definitions

Definition 6.1.1. Let R be a ring. A left R-module is an abelian group M, written additively, along with map $R \times M \to M$ called scalar multiplication and denoted $(r, m) \mapsto rm$. The map must follow certain properties:

1. $r(m_1 + m_2) = rm_1 + rm_2$
2. $(r_1 + r_2)m = r_1m + r_2m$
3. $(r_1r_2)m = r_1(r_2m)$
4. $1m = 1$

We can define left R-modules similarly. If R is commutative then left and right modules are the same (which is non-trivial) and then we call them R-modules.

Proposition 6.1.1. *1.* $0m = 0_M = r0$

2. $-(rm) = (-r)m = r(-m)$

Example 6.1.1. If R is a field, then R-modules are vector spaces. $\mathbb{Z}$-modules are exactly abelian groups. This is because $1m = m$ gives us only one way to define xm for any $x \in \mathbb{Z}$ so the scalar map is uniquely defined.

Remark. Let R be a ring, consider R° the opposite ring where addition is defined in the usual way $r^\circ + s^\circ = (r + s)^\circ$ and $r^\circ s^\circ = (sr)^\circ$. Then, a left R-module is a right R$^\circ$-module.

Example 6.1.2.

1. Ideals in R are R-modules. In particular, R is an R-module over itself.
2. Let $f : R \to S$ be a ring homomorphism. If M is an S-module, we can pull it back to an S-module with the multiplication rule $sm = f(s)m$.
3. Let M be an abelian group. Consider $R = End(M)$ which is a ring since M is abelian so functions can be added and composed. As it turns out, M is an End(M)-module. We can take $End(M) \times M \to M$ as $(f, m) \mapsto f(m)$.

Let M be a left R-module. We want to construct $f : R \to End(M)$ such that $r \mapsto (f(r) : m \mapsto rm)$. By (M1), $f(r)(m_1 + m_2) = f(r)(m_1) + f(r)(m_2)$ so $f(r) \in End(M)$. By (M2) $f(r_1 + r_2)(m) = f(r_1)(m) + f(r_2)(m)$ so that $f(r_1 + r_2) = f(r_1) + f(r_2)$. By (M3) $f(r_1r_2)(m) = f(r_1)(f(r_2)(m)) = f(r_1) \circ f(r_2)(m)$ so $f(r_1r_2) = f(r_1)f(r_2)$. By (M4) $f(1)(m) = m$ so $f(1) = 1$. The axioms of

scalar multiplication give exactly the necessary conditions for f being a ring homomorphism.
Conversely, if we are given some $f : R \to End(M)$, we know that M is an End(M)-module. So, we can pullback via f to M being an R-module. As a result, given M an abelian group and R a ring, we have a bijection {set of R-module} $\cong Hom_{Rings}(R, End(M))$.

In more categorical terms, fix M. We can define a functor $F : Rings^{\circ} \to Sets$ that takes a ring R to the set of all R-module structures on M. By the above, this functor is corepresented by $End(M)$.

6.2 R-linear maps

Let M and N be two R-modules. A group homomorphism $f : M \to N$ can be extended to an R-linear map such that $f(rm) = r(fm)$. This lets us create categories $RMod$ and $ModR$. These are abelian categories.

First, we exhibit products and coproducts.

Let $(M_i)_{i \in I}$ be a family of R-modules. $\prod_{i \in I} M_i$ where $r(m_i) = (rm_i)$. On the other hand, we define coproducts as $\coprod_{i \in I} M_i = \{(m_i) \in \prod M_i : \text{almost all } m_i \text{ are zero}\}$.

Next, we show that we have kernels and cokernels. We call $N \subset M$ a subgroup if $RN \subset N, N$ is an R-module, a submodule. Given $f : M \to N$ we can see that easily that $ker(f) \subset M$ is a submodule and $Im(f) \subset N$ a submodule. We define $Coker(f) = N/Im(f)$ where a quotient module is just a quotient group with $r(m + N) = rm + N$. It can be checked that this is well-defined. The first isomorphism theorem carries over to modules.

6.3 Internal product

Suppose M is an R-module and $(M_i)_{i \in I}$ a family of submodules. By composing each inclusion $M_i \to M$, we get the map $\coprod_{i \in I} M_i \to M$ where $(m_i) \mapsto \sum m_i$. This sum is well-defined due to the finiteness condition on coproducts.

7 Exact sequences of modules

7.1 Short exact sequences

A short sequence $0 \longrightarrow N \xrightarrow{i} M \xrightarrow{j} P \longrightarrow 0$. of R-modules is exact $\iff$ it is exact as groups. Then, $N \cong Im(i) \subset M$ and $P \cong M/Im(i) \cong M/N$.

Let's now fix R. We can the consider the category of short exact sequences with objects short exact sequences and triples (α, β, γ) that make the following diagram commutative.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \xrightarrow{i} & M & \xrightarrow{j} & P & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & N' & \xrightarrow{i'} & M' & \xrightarrow{j'} & P' & \longrightarrow & 0 \end{array}$$

In particular, (α, β, γ) is an isomorphism $\iff$ α, β, γ are all isomorphisms.

Example 7.1.1. Every short exact sequence is isomorphic to some standard short exact sequence.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \xrightarrow{i} & M & \xrightarrow{j} & P & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathbb{R}} & & \downarrow{\scriptstyle 1_M} & & \downarrow{\scriptstyle \mathbb{R}} & & \\ 0 & \longrightarrow & Im(i) & \longrightarrow & M & \longrightarrow & M/Im(i) & \longrightarrow & 0 \end{array}$$

Therefore, to prove a certain property of short exact sequences, it suffices to do so for arbitrary short exact sequences.

7.2 Splitting of short exact sequences

Proposition 7.2.1. *Let* $0 \longrightarrow N \xrightarrow{f} M \xrightarrow{g} P \longrightarrow 0$ *(*) be a short exact sequence. TFAE:*

1. *g splits i.e. $\exists g' : P \to M$ such that $g \circ g' = 1_P$.*
2. *f splits i.e. $\exists f' : M \to N$ such that $f' \circ f = 1_N$.*
3. *(*) is isomorphic to* $0 \longrightarrow N \longrightarrow N \oplus P \longrightarrow P \longrightarrow 0$

Proof. (1) $\Rightarrow$ (3): Assume that g splits via g'. We can then construct the morphism which commutes since g' is the splitting of g. The left and right

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \longrightarrow & N \oplus P & \longrightarrow & P & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle 1_N} & & \downarrow{\scriptstyle h=(f,g')} & & \downarrow{\scriptstyle 1_P} & & \\ 0 & \longrightarrow & N & \xrightarrow{f} & M & \xrightarrow{g} & P & \longrightarrow & 0 \end{array}$$

morphisms are isomorphisms. It can be shown that this implies the central h is also an isomorphism. By the snake lemma

$0 \to ker(1_N) \to ker(h) \to ker(1_P) \to coker(1_N) \to coker(h) \to coker(1_P) \to 0$ is an exact sequence. By noting that $1_N, 1_P$ are isomorphisms so they have trivial kernels and cokernels, we get $ker(h) = 0$ and $coker(h) = 0$ so h is also an isomorphism.

(2) $\Rightarrow$ (3): This follows in the same way where we now take $h = (f'g) : M \to N \oplus P$ and the isomorphism follows again by the snake lemma.
(3) $\Rightarrow$ (1) and (2): Once we are given the isomorphism, we can easily find a splitting $g' : p \mapsto (0, p), f' : (n, p) \mapsto n$ $\square$

8 Free modules

8.1 Definitions

Definition 8.1.1. Let F be an R-module. A subset $X \subset F$ is called a basis for F if $\forall f \in F : \exists!(a_x)_{x \in X}$ such that almost all a_x are zero and $f = \sum a_x x$. Every module that has at least one basis is called free.

Remark. This definition closely follows the one from linear algebra. However, we will see later that not all properties are inherited. In particular, we cannot always define the rank of a free module as we may have bases of different cardinalities for the same free module.

Example 8.1.1.

1. Let R be a field. Then, every R-vector space is a free R-module.
2. $R^n = R \oplus \cdots \oplus R$ is a free module with basis $\{e_i\}_{i \in I}$ where e_i is the idempotent defined earlier.
   In fact, this is the canonical example of a free module. Consider an arbitrary F free R-module with basis $X \subset F$. Then, we have an isomorphism $f : R^{(X)} = \coprod_{x \in X} R \to F$ given by $(a_x)_{x \in X} \mapsto \sum a_x x$. That f is an isomorphism follows directly from the definition.
3. Let $R = \mathbb{Z}$. Free abelian groups have no torsion (elements of finite order). $\mathbb{Z}^{(X)}$ is torsion free. However, the converse is not true. For example, $\mathbb{Q}$ is not free and has no torsion. Therefore, if a $\mathbb{Z}$-moudle has torsion, it's not free.
4. There exists rings R such that $R \cong R^2 \cong R^3 \cong \cdots$ as R-modules. However, if R is commutative, then $R^m = R^n$ then $n = m$. So, for a commutative ring, we can define $rank(F) = \#$basis elements. Even for non-commutative if $\exists h : R \to D$ where D is a division ring, then the rank of F is well-defined.

8.2 Categorical properties

Recall that we can identify $X \subset R^{(X)}$ using the map $x \mapsto \delta_x$ where $\delta_x(x')$ is defined using the Kronecker-Delta function. We can extend this property to any free module. Let X be a set, M any R-module and consider $f : X \to M$. Then, $\exists!$ R-linear map $g : R^{(X)} \to M$ such that $g(x) = f(x)$ given by $g(x) = g(\sum a_x x) = \sum a_x f(x)$. This gives us a bijection $Maps(X, M) \cong$

$Hom(R^{(X)}, M)$. Therefore, this gives another free functor that is left-adjoint to forget.

Let F be an R-module and consider the functor represented by F

$$\begin{aligned} RMod &\to AbGroups \\ M &\mapsto \mathrm{Hom}(F, M) \end{aligned}$$

In general, this functor maps onto the category of sets. However, since M is an abelian group, $\mathrm{Hom}(F, M)$ is also an abelian group. In general, the Hom-functor is left exact.

Corollary 8.0.1. *This functor is exact if F is free.*

Proof. We need to show right exactness. It suffices to show that in the diagram below, we can lift the map $f : F \to P$ to a map $g : F \to M$.

$$\begin{array}{ccccccccc} & & & & & & F & & \\ & & & & & \overset{\exists g}{\swarrow} & \downarrow{\scriptstyle f} & & \\ 0 & \longrightarrow & N & \longrightarrow & M & \xrightarrow{h} & P & \longrightarrow & 0 \end{array}$$

If F is free, then we can write $F = R^{(X)}$ and then f corresponds to some $\tilde{f} : X \to P$. Then, we can look at $f(x) \in P$ which must be equal to some $h(m), m \in M$. We can then construct g as follows: $\forall x \in X : x \mapsto m$ as described above. Since F is free, this extends to $g : F \to M$ an R-linear map. □

Remark. We want to understand $\mathrm{Hom}(R^n, R^m)$. First, note that $\mathrm{Hom}(R, R) \cong R$ as linear maps since each element $a \in R$ uniquely defines the map $h : x \mapsto xa$. Now, we use the additivity of Hom to write $\mathrm{Hom}(R^n, R^m) \cong (\mathrm{Hom}(R, R^m))^n \cong (\mathrm{Hom}(R, R))^{nm} \cong R^{nm}$ which is exactly the set of $m \times n$ matrices with coefficients in R.

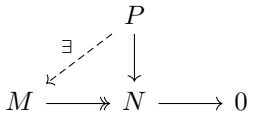
9 Projective and Injective modules

9.1 Projective modules

Proposition 9.1.1. *Let P be an R-module. Then TFAE:*

1. *The functor $\mathrm{Hom}_R(P, -) : RMod \to AbGroups$ is exact.*
2. *Every diagram of the form shown below extends to a commutative diagram.*

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow & & \\ M & \twoheadrightarrow & N & \longrightarrow & 0 \end{array}$$



3. *Every short exact sequence* $0 \longrightarrow A \longrightarrow B \longrightarrow P \longrightarrow 0$ *is split.*

Definition 9.1.1. P is called projective if (1), (2) and (3) hold.

Example 9.1.1. Free R-modules are projective.

Remark. Every R-modules is isomorphic to the factor module of a free module.

Proof. Let M be an R-module. Pick $X \subset M$ a set of generators: $\forall m \in M : m = \sum a_x x$ for some sequence $(a_x)_{x \in X}$. Then, the inclusion $X \hookrightarrow M$ gives us a linear-map map $f : R^{(X)} \twoheadrightarrow M$ which is surjective since X generates M. Therefore, $M \cong F/\ker(f)$. □

Proposition 9.1.2. *An R-module is projective if and only if P is a direct summand of a free module i.e. $\exists Q : P \oplus Q$ is free.*

Proof. $\Rightarrow$ Assume that P is projective. We can write $P \cong F/N$ for F free by the above remark. Then, we can construct the sequence $0 \longrightarrow N \longrightarrow F \longrightarrow P \longrightarrow 0$. By the above properties of a projective module, this sequence splits so $F = N \oplus P$.
$\Leftarrow$ Assume that $P \oplus Q = F$ is free. Consider the functor $\alpha_N(M) = Hom_R(N, M)$ represented by some module N. Then, α_F is exact since F is free (therefore, projective). In the category of functors, $\alpha_F = \alpha_P \oplus \alpha_Q$. Therefore, α_P, α_Q are exact. This imples that P, Q are projective. □

Can we find examples of modules that are projective but not free?

Example 9.1.2.

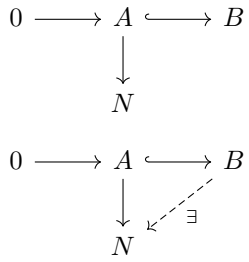
1. Let $R = R_1 \times R_2$. Consider $P = R_1 \times 0, Q = 0 \times R_2$ as R-modules. By construction $R = P \oplus Q$ which is free. Therefore, P, Q are projective. However, these are not free. Assume that $P = R_1 \times 0$ has a basis B. Let $(r, 0) \in B$. Then, $(0, 0) = (0, 0) \cdot (r, 0) = (0, 1) \cdot (r, 0)$ which means that the representation is not unique so it's not a basis. Therefore, it is not free.
2. Example from topology $R = \mathbb{R}[x, y, z]/\langle x^2 + y^2 + z^2 - 1 \rangle$. Omitted.

9.2 Injective modules

Proposition 9.2.1. *Let N be a left R-module. Then TFAE:*

1. *The functor* $\mathrm{Hom}(N, -)$ *is exact.*

2. *Every diagram of the form below can be extended as shown to a map from a larger module.*



3. *Every sequence* $0 \longrightarrow N \longrightarrow X \longrightarrow Y \longrightarrow 0$ *is split.*

Example 9.2.1. Injective $\mathbb{Z}$-modules are precisely divisible abelian groups. N is divisible if $\forall n \in \mathbb{Z} : n \neq 0 \Rightarrow nN = N$. For example, $\mathbb{Q}, \mathbb{Q}/\mathbb{Z}, \mathbb{R}, \mathbb{R}/\mathbb{Z}$.

10 Tensor products

The setting here is that we pick a ring R and two modules M and N where M is a right R-module and N is a left R-module. We denote this $(M_R, {}_RN)$.

10.1 Definitions

Definition 10.1.1. Let A be an abelian group written additively. A bilinear map from $M \times N$ to A is a map $B : M \times N \to A$ such that:

1. $B(m_1 + m_2, n) = B(m_1, n) + B(m_2, n)$
2. $B(m, n_1 + n_2) = B(m, n_1) + B(m, n_2)$
3. $B(mr, n) = B(m, rn)$

We use $Bil(M, N; A)$ to denote the set of all bilinear maps from $M \times N$ to A. Since A is an abelian group, this set is also an abelian group. Given $h : A \to A'$ we can compose $h \circ B : M \times N \to A'$. This composition gives us a map $h_* : Bil(M, N; A) \to Bil(M, N; A')$.

The property above gives rise to a functor. Fix $(M_R, {}_RN)$. Consider $F : AbGroups \to AbGroups$ that takes $A \mapsto Bil(M, N; A)$. In fact, this is an additive functor. A natural question is whether this functor is representable by some object in *AbGroups*. We will show that such an object does exist. We define it to be the tensor product.

Definition 10.1.2. The tensor product $M \otimes_R N$ is the abelian group representing the functor above. In other words, $\mathrm{Hom}(M \otimes_R N, A) \cong Bil(M, N; A)$.

Remark. The tensor product is determined uniquely upto canonical isomorphism. Therefore, we don't even need to consider the elements of the tensor product (except to prove its existence).

Remark. Recall that to have a functor that represents this is to have a natural isomorphism between $\mathrm{Hom}(M \otimes_R N, -)$ and $Bil(M, N; -)$ i.e. for any $A \in AbGroups$, we have a bijection $\mathrm{Hom}(M \otimes_R N, A) \cong Bil(M, N; A)$.

10.2 Universal properties of tensor product

We will now look at some universal properties that this construction gives us. Our motivation here is that the identity map $1_{M \otimes_R N} \in \mathrm{Hom}(M \otimes_R N, M \otimes_R N)$ i.e. when A is set to $M \otimes_R N$ must be mapped to some unique bilinear map $B_{univ} : M \times N \to M \otimes_R N$. Further, this construction is universal in the sense that if we now take an arbitrary A and some $B \in Bil(M, N; A)$ then this corresponds to some $f \in \mathrm{Hom}(M \otimes_R N, A)$ i.e. $f : M \otimes_R N \to A$. This f can be viewed as the result of applying $f_* : \mathrm{Hom}(M \otimes_R N, M \otimes_R N) \to \mathrm{Hom}(M \otimes_R N, A)$ to $1_{M \otimes_R N}$. It is clear that $f_*(1_{M \otimes_R N}) = f \circ 1_{M \otimes_R N} = f$. But the advantage of viewing things this way is that, via the commutative diagram below, we also get that $B(m, n) = f \circ (B_{univ}(m, n))$. To simplify the notation a bit, we write $B_{univ}(m, n) = m \otimes n$ so that $B = f(m \otimes n)$.

$$\begin{array}{ccc} B \in Bil(M, N; A) & \xrightarrow{\sim} & \mathrm{Hom}(M \otimes_R N, A) \ni f \\ {\scriptstyle f_*}\uparrow & & {\scriptstyle f_*}\uparrow \\ B_{univ} \in Bil(M, N; M \otimes_R N) & \xrightarrow{\sim} & \mathrm{Hom}(M \otimes_R N, M \otimes_R N) \ni 1 \end{array}$$

It is worth appreciating what we have done here. We saw that bilinear maps serve as a nice functor between abelian groups. If we take the abelian group $M \otimes_R N$ that represents this functor, then we can use its universal properties to rewrite every bilinear $B : M \times N \to A$ in terms of a unique group homomorphism $f : M \otimes_R N \to A$ such that $B(m, n) = f(m \otimes n)$.

Remark. Since $m \otimes n$ is really just $B_{univ}(m, n)$ all properties of a bilinear map hold:

1. $(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n$
2. $m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2$
3. $mr \otimes n = m \otimes rn$

10.3 Existence of tensor product

All these properties are really convenient but essentially useless unless we can verify for sure that this functor is representable. We will give a constructive proof by creating an abelian groups that satisfies the required properties.

Proposition 10.3.1. *Tensor products exist.*

Proof. Fix (M, N) and consider $F = \mathbb{Z}^{(M\times N)} = \{\sum a_{m,n} \cdot (m, n)\}$ the free $\mathbb{Z}$-module (abelian group) generated by the set $M \times N$ where we momentarily forget the structure of M, N as R-modules.
Consider the subgroup $H \subset F$ generated by all elements of the form:

1. $(m_1 + m_2, n) - (m_1, n) - (m_2, n)$
2. $(m, n_1 + n_2) - (m, n_1) - (m, n_2)$
3. $(mr, n) - (m, rn)$

Next, quotient this subgroup out of F to get F/H. In this group, all elements of the above form get sent to 0 so the axioms of a bilinear map hold (if we consider taking a tuple as an operation). We make this more concrete now.
We claim that $M \otimes_R N = F/H$ so we need to check that the universal property holds. First, we need a natural universal map $B_{univ} : M \times N \to F/H$. We don't have much choice in defining this map so we define in the expected way $(m, n) \mapsto \overline{(m, n)}$. This map being bilinear is exactly the same as the H being generated by the elements specified above.
We are only left to show the universal property $Bil(M, N; A) \cong \mathrm{Hom}(F/H, A)$. A group homomorphism $f : F/H \to A$ corresponds to a group homomorphism $g : F \to A$ with $g(H) = 0$. Since F is generated by $M \times N$ this is the same as giving a map from the basis $B : M \times N \to A$ where the map is bilinear if and only if $B(H) = 0$. □

Corollary 10.0.1. *In the above construction, we saw that $M \otimes_R N$ is free and was constructed by elements of the form $\overline{(m, n)} = B_{univ}(m, n) \in F/H$. In general, it is generated by $m \otimes n$.*

Example 10.3.1.

Consider the tensor product $M \otimes_R R$. This represents the functor $Bil(M, R; A)$. So, let's try and understand bilinear maps of this form. Let $B : M \times R \to A$ be a bilinear map. Then $B(m, r) = B(mr, 1)$. In this map, if we fix the second variable to $1 \in R$, then we get a map $f : M \to A$ which turns out to be a group homomorphism because $B(m_1+m_2, 1) = B(m_1, 1)+B(m_2, 1)$ i.e. $f(m_1+m_2) = f(m_1)+f(m_2)$. Recall that any bilinear map $B(m, r) = B(mr, 1) = f(mr)$ so it is completely described by a group homomorphism $f : M \to A$. In other words, we have the bijection $Bil(M, R; A) \cong \mathrm{Hom}(M, A)$. So, $M \otimes_R R = M$. Similarly, $N \otimes_R R = N$.

10.4 Tensor bifunctor

Consider two pairs of modules M, N and M', N' as well as group homomorphisms $f : M \to M', g : N \to N'$. We want to construct a canonical group homomorphism $M \otimes_R N \to M' \otimes_R N'$. It seems appropriate to then call this map $f \otimes g$. By canonical, we mean that $(f \otimes g)(m \otimes n) = f(m) \otimes g(n)$. Without getting too caught up in notation, this means that first applying the universal map B_{univ} and then mapping it under $f \otimes g$ is the same as first mapping each

individually and then applying the universal map B'_{univ}.
Again, there is a natural construction here which turns out to work. By now, we should be familar with the interplay between group homomorphisms from the tensor product $M \otimes_R N$ and bilinear maps from $M \times N$. With this in mind, it is natural to start by trying to construct a bilinear map $B : M \times N \to M' \otimes_R N'$. We have only one way of sending elements of $M \times N$ to $M' \times N'$ and the universal map gives us a way of mapping $M' \times N' \to M' \otimes_R N'$. Composing this gives us a formula for $B : (m, n) \to f(m) \otimes g(n)$. It remains to check whether this map is bilinear but the check is almost trivial as we are composing a group homomorphism with another bilinear map. Now that we have a bilinear map, we know that is must factor through the tensor product $M \otimes_R N$. In particular, there exists a unique group homomorphism $h : M \otimes_R N \to M' \otimes_R N'$ such that $h(m \otimes n) = f(m) \otimes g(n)$. This is the required $f \otimes g$.

With this construction, we have a bifunctor $F : ModR \times RMod \to AbGroups$ that maps $(M, N) \to M \otimes_R N$ and $(f, g) \to f \otimes g$. This functor is bi-additive but not additive. This means that if we fix one argument, then the resulting functor is additive.

10.5 Exactness of bilinear functor

Omitted. Check end of Lec 11 notes.

10.6 Hom-tensor adjunction

Fill in later. Start of Lec 12 notes.

11 Finitely generated modules over PID

In linear algebra, we have successfully classified all finitely generated modules over a field F (known as vector spaces) as isomorphic to a finite number of copies of F. This is possible because of nice properties of fields. In this section, we ease the restriction on our ring and only instead that it is a PID such as $\mathbb{Z}$ or $F[x]$. As it turns out, it is possible to get a general classification here but the process is much more involved.

11.1 Torsion modules

We start by focusing on how PIDs differ from fields. For this section, let R be a PID and M a module. In a vector space, multiplication by a non-zero scalar cannot send a non-zero vector to 0. However, in an abelian group (which is a Z-module) such as a cyclic group, the order of an element a is an example of an integer $n \in \mathbb{Z}$ such that $na = 0$. This motivates the next definition.

Definition 11.1.1. We call $m \in M$ a torsion element if $am = 0$ for some $a \neq 0 \in R$.

For example, every element of an cyclic group is a torsion element. It is easy to check that $M_{tors} = \{m \in M : m \text{ torsion } \} \subset M$ is a submodule. If $M = M_{tors}$ then we call M a torsion module, if $M_{tors} = 0$, we say that M is torsion-free. It follows that M/M_{tors} is always torsion-free. We are interested in this construction as free modules are torsion free (since $F = \coprod R$, each R torsion free.) This case is then closer to the world of vector spaces.

Proposition 11.1.1. *Let F be a free module of finite rank (finitely generated). Let $M \subset F$ be a submodule. Then, M is also free with $rank(M) \leq rank(F)$.*

Proof. Since we are given that F has finite rank, say n with basis $B = \{x_1, \ldots, x_n\}$ we can use induction on n. The base case is true since if $rank(F) = 1$ then $F = R$ and all submodules are ideals $I \subset R$. Since R is principal, $rank(I) = 1$. Assume the inductive hypothesis for $n-1$. Let F be a free module of rank n. Consider the projection onto the n^{th} variable $\pi_n : F \to R$ where $\sum a_i x_i \mapsto a_n$ which is clearly an R linear map that is surjective with $\ker(f)$ also free with basis $B' = \{x_1, \ldots, x_{n-1}\}$. Now if we consider any other submodule $M \subset F$, its image $f(M)$ must be an ideal in R. Again, we use the fact that R is a PID so $f(M) = cR$ for some $c \in R$. Now the map $f|_M : M \to cR$ is surjective and has kernel $\ker(f) \cap M \subset \ker(f)$ a submodule. Then we get an exact sequence $0 \longrightarrow \ker(f) \cap M \longrightarrow M \longrightarrow cR \longrightarrow 0$ which splits since cR is free (so projective). Therefore $M = \ker(f) \cap M \oplus cR$. By the inductive hypothesis, $rank(\ker(f) \cap M) \leq rank(\ker(f)) = n - 1$. Therefore, $rank(M) \leq n - 1 + 1 = n$. □

Remark. If we have a M an R-module, then $S^{-1}M$ is a $S^{-1}R$-module. Further, the inclusion map $f : M \to S^{-1}M$ is R-linear (when the localized module is viewed as a module over the original ring R) so $M_{tors} = \ker(f)$. So, we can view M as an R-submodule of $S^{-1}M$ is M is torsion free. Check end of Lec 12 notes for details.

11.2 Classification

Proposition 11.2.1. *Every finitely generated torsion free module over a PID is free.*

Proof. Let M be a finitely generated torsion free module over a PID. Since M is finitely generated, we can write it as $M = \sum_{j=1}^{k} Rm_j$. We will now make use of the earlier remark. Let K denote the quotient field of R. Since we are given that M is torsion free we have inclusion $M \hookrightarrow S^{-1}M$ as R-modules. Recall that $S^{-1}M$ is a vector space over K. Therefore, it has some basis $B = \{x_1, \ldots, x_n\}$. Consider $F = \sum_{i=1}^{n} Rx_i \subset S^{-1}M$ which is a free R-module with same basis B.

It is clear that it suffices to show that $M \subset F$ is an R-submodule as we just proved that the submodule of a free module is also free. Since M. Each m_j is clearly a linear combination of x_i with coefficients in K (since its the basis of a vector space). Then, $\exists a_j \neq 0 \in R$ such that $a_j m_j \in F$ i.e. we can scale each m_j by some $a_j \in R$ to get it in F. If we consider $a := \prod a_j$ then each $am_j \in F$. And since (m_j) generates M, we have $aM \subset F$ a free module. Further, we have the isomorphism $M \overset{a}{\cong} aM$ where its trivial kernel follows from the fact that M is torsion-free. Therefore, $M \subset F$. □

Remark. Let R be a PID, M a finitely generated module, consider $M_{tors} \subset M$. We get the short exact sequence $0 \longrightarrow M_{tors} \longrightarrow M \longrightarrow M/M_{tors} \longrightarrow 0$. Since M/M_{tors} is torsion-free, it is free therefore the sequence splits. So, $M = M_{tors} \oplus M/M_{tors}$ and the second summand is free. So it suffices to classify torsion modules.

Definition 11.2.1. Let $O \neq P \subset R$ be a prime module i.e. $P = pR$ for some prime element $p \in R$. Let M be a torsion finitely generated module. We define $M(P) = \{m \in M : p^n m = 0 \text{ for some } n > 0\}$ which we call the P-primary submodule of M.

Lemma 11.1. *Let $a_1 \dots a_n$ be relatively prime elements in a PID R. Then, $\exists b_1, \dots, b_n \in R : a_1 b_1 + \cdots + a_n b_n = 1$.*

Proof. Since R is a PID, $I = \sum a_i R = cR$ for some $c \in R$. As a result, each $a_i R \subset cR$ so $\forall i : c | a_i$. But since all a_i are relatively prime, we have that $c \in R^\times$ i.e. $I = R$. This completes the proof as $1 \in R$. □

Remark. This is not true if R is not a PID. For example, consider $\mathbb{Z}[x_1, \dots, x_n]$ with $a_i = x_i$. Then, $\sum x_i R$ is an ideal without any constant terms.

Corollary 11.1.1. *Let M be an R-module, $m \in M$ such that a set of relatively prime elements a_i are such that $a_i m = 0$. Then, $m = 0$.*

Proof. We have $\sum a_i b_i = 1$. Then, $m = \sum a_i b_i m = \sum 0 = 0$. □

Theorem 11.2. *Let M be a finitely generated torsion module over a PID R. Then, $M = \coprod_{P \subset R} M(P)$ where almost all $M(P)$ are zero.*

Proof. Check middle of Lec 13. □

Remark. Let R be a commutative ring, M and R-mdoule with $I \subset R$ an ideal such that $IM = 0$. Then M also have a structure as an R/I-module: $(a+I)m = am$. This can be viewed as an application of the change of ring functor.

Let $0 \neq P \subset R$ be a prime ideal, $P = pR$ and let M be an R-module such that $PM = 0 \iff pM = 0$. Then, we can view M as an R/P-module. Note that in a PID R, R/P is a field since P is maximal over principal ideals so it is maximal in the ring.

Example 11.2.1. M/PM is a vector-space over R/P since $P(M/PM) = 0$. Define ${}_pM = \{m \in M : pm = 0\}$. Then ${}_pM$ is a vector space over R/P.

Lemma 11.3 (key lemma)**.** *Let M be a module over R a PID and $p \in R$ a prime such that $p^n M = 0$ for some $n > 0$ but $p^{n-1}M \neq 0$. Further, if we assume that $\dim_{R/P}({}_pM) = 1$. Then $M \cong R/p^nR$.*

Proof. Lec 14 □

Skipped section on length of a torsion module that helps us prove the following theorem.

Theorem 11.4. *A finitely generated module M over a PID R is a unique direct sum of cyclic modules R and R/P^n.*

11.3 Invariant factors and elementary divisors

Skipped, check Lec 15 and 16 for classification of abelian groups, Rational Canonical Form and Jordan Normal Form.

Part III

Fields

12 Field extensions

Fields are the simplest type of rings as the category of modules over fields is just vector spaces which are easy to classify upto isomorphism.

12.1 Introduction to fields

The category of fields has as objects fields and arrows field homomorphisms, which are the same as ring homomorphism. Note that every $f : K \to L$ is injective. This is because $\ker(f) \subset K$ an ideal but the only ideals of K are 0 and K. If the kernel were all of K, then we would not have $f(1) = 1$ which is required for ring homomorphisms. Therefore, $\ker(f) = 0$.

Definition 12.1.1. Let $K \subset L$ be a subfield. Then we say that L is a field extension of K and denote it L/K.

Remark. This notation is consistent as L is a vector space over K. This is because L is a vector space over itself and the inclusion map $i : K \to L$ lets us pull-back every vector space over L to a vector space over K. We denote $[L : K] = \dim(L/K)$.

Example 12.1.1.

1. $\dim(L/K) = 1 \iff L = K$
2. $\mathbb{C}/\mathbb{R}$ has basis $\{1, i\}$ so $[\mathbb{C} : \mathbb{R}] = 2$
3. $[\mathbb{R} : \mathbb{Q}] = \infty$

Proposition 12.1.1. *Let $L/K/F$ be field extensions. Then $[L : F] = [L : K][K : F]$.*

Proof. Let (x_i) be a basis for L/K and (y_j) a basis for K/F. Then $(x_i y_j)$ is a basis for L/F. Assume $\sum_{ij} a_{ij} x_i y_j = 0$. Then $\sum_j (\sum_i a_{ij} x_i) y_j = 0$ and by linear independence of y_j, for each j we get that $\sum_i a_{ij} x_i = 0$. It follows from linear independence of (x_i) that each $a_{ij} = 0$. Let $a \in L$. Then $a \in span(y_j)$ and each $y_j \in span(x_i)$ so $a \in span(x_i y_j)$. □

Corollary 12.0.1. *Both $[L : K]$ and $[K : F]$ divide $[L : F]$*

Corollary 12.0.2. *By induction, if we have $F_0/F_1/\cdots/F_n$ then $[F_0 : F_n] = \prod_{i=0}^{n-1} [F_i : F_{i+1}]$*

12.2 Subfields

We now consider the notion of generating another field from a set over a smaller field. In particular, let K/F be a field extension and consider $S \subset K$ a field extension. We wish to construct the smallest field containing S that lies in between K and F. This is $F \subset \bigcap_{F \subset K' \subset K, S \subset K'} K' \subset K$. For $S = \{\alpha_1, \ldots, \alpha_n\}$ we write this intersection as $F(\alpha_1, \ldots \alpha_n)$. Pay attention to the brackets used here! Explicitly, we can write this as the set of all fractions of functions in $F[x_1, \ldots, x_n]$ evaluated at $x_i = \alpha_i$.

We have $F[\alpha_1, \ldots, \alpha_n] \subset F(\alpha_1, \ldots, \alpha_n)$ where the inclusion is an equality if and only if $F[\alpha_1, \ldots, \alpha_n]$ is a field (it is always a subring).

Example 12.2.1.
1. $\mathbb{C} = \mathbb{R}[i] = \mathbb{R}(i)$
2. $F \subset F[x] \subset F(x)$

Definition 12.2.1. Consider K/F a field extension and $\alpha \in K$. We say that α is algebraic over F if $\exists f \in F[x]$ nonzero such that $f(\alpha) = 0$. K/F is an algebraic field extension if every $\alpha \in K$ is algebraic over F.

Example 12.2.2.
1. Let K/F. All $a \in F$ are algebraic over F as it is a root of $(x - a) \in F[x]$
2. $\mathbb{C}/\mathbb{R}$ is a field extension as $z = a + bi$ solves $z^2 - 2az + a^2 + b^2 = 0$
3. Let $L/K/F$. $\alpha \in L$ is algebraic over $F \Rightarrow \alpha$ is algebraic over K.
4. If $\alpha \in K/F$ is transcendental then $F[x] \cong F[\alpha]$ via $x \mapsto \alpha$ which is a ring homomorphism and surjective in general, injective by definition of α being transcendental. In particular, then $F[\alpha]$ is not a field.

As it turns out, the converse of the last point is also true.

Theorem 12.1. *Let $\alpha \in K/F$ be algebraic over F. Then:*

1. *$\exists!$ irreducible monic polynomial $m_\alpha(\alpha) \in F[x] : m_\alpha(\alpha) = 0$. We call m_α the minimal polynomial of α.*
2. *If another polynomial f kills α then $m_\alpha | f$ in $F[x]$.*
3. *$F[\alpha] = F(\alpha) \cong F[x]/m_\alpha F[x]$ so it is a field.*
4. *The set $B = \{1, \alpha, \ldots, \alpha^{n-1}\}$ where $n = \deg(m_\alpha)$ is a basis for $F(\alpha)/F$.*

Proof. Lec 18 □

To find the degree of an algebraic extension, it suffices to find a polynomial that solves it and then reduce it to an irreducible.

Example 12.2.3.
1. Consider $\sqrt{2} \in \mathbb{C}/\mathbb{Q}$, $\deg(\sqrt{2}) = 2$ since $x^2 - 2$ is irreducible.

2. Let p be a prime. We define the primitive root of degree p as $x \in \mathbb{C}/\mathbb{Q}$ such that $x^p = 1$ but $x \neq 1$. We can factor $x^p - 1 = (x-1)(x^{p-1} + \cdots + x + 1)$. Since $x \neq 1$ we must have x solves the second factor. By a modification of the Eisenstein criterion, we prove that it is irreducible. So, $[\mathbb{Q}(x) : \mathbb{Q}] = p - 1$.

Remark. This is not true for $p \neq$ prime.