Math 110BH Notes

Nathan Solomon

March 6, 2024

Contents

1 1/8/2024 lecture

1.1 Definition of a ring

A *ring* is a set R with two operations, *addition* and *multiplication*, such that

- $(R, +)$ is an abelian group
- *Left & right distibutivity* – For any $a, b, c \in R$, $(a+b)c = ac+bc$ and $c(a+b) = ca+cb$
- *Associativity* – $(ab)c = a(bc)$
- *Unitarity* – There exists an element called 1 such that $1a = a = a1$ for any $a \in R$

Sometimes people leave of those last two criteria, but in this class, we will only talk about associative, unital ring.

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

1.2 Examples of rings

The simplest ring is the zero ring, which is the zero group with $1 = 0$.

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, and $\mathbb{Z}/n\mathbb{Z}$ are all commutative rings.

If R is a ring, then $M_n(R)$, the set of $n \times n$ rings over R where $n \in \mathbb{N}$, is a ring. If R is not the zero ring and $n > 1$, then $M_n(R)$ is noncommutative.

If $(A, +)$ is an abelian group and $R = \text{End}(A) = \{f : A \to A \text{ is a homomorphism}\}$ is the set of endomorphisms of A, then R becomes a ring when you define addition by $(f + g)(a) = f(a) + g(a)$ and define multiplication to be composition of endomorphisms.

For any ring $R = (R, +, \cdot)$, there exists another ring, $R^{op} = (R, +, *)$, defined by $a * b := b \cdot a$.

If R is a ring, then $R[x]$ (the set of polynomials in the variable x over R) is also a ring. If R is commutative, then so is $R[x]$. In this case, "polynomials" are essentially lists of coefficients, with addition and multiplication defined the way you would expect for polynomials. This can be generalized to a finite set X of variables – in that case, $R[X]$ is the set of polynomials over the variables in X, which are assumed to commute with each other.

If R is a ring and X is a set, then $S := \{f : X \to R\}$ with the operations defined by $(f + g)(x) = f(x) + g(x)$ and $(f \cdot g)(x) = f(x) \cdot g(x)$ forms a ring. If $|X| = 1$, then $R = S$.

1.3 Properties of rings

- $0a = 0 = a0$
- $(-a)(b) = -(ab) = (a)(-b)$
- A nonzero element a of a commutative ring is called *invertible* (or is sometimes called a *unit*) iff there exists a nonzero element $b \in R$ such that $ab = 1 = ba$. If b exists, it is unique, and it is called the *inverse* of a.
- If a and b are both invertible, then $(ab)^{-1} = b^{-1}a^{-1}$.

1.4 The multiplicative group

If R is a commutative ring, let $R^\times$ be the set of invertible elements in R. Then $R^\times$ is a multiplicative group. R is called a *field* iff it is commutative, R is not the zero ring, and $R^\times = R\backslash\{0\}$. $\mathbb{Q}$ and $\mathbb{R}$ are examples of fields.

Here are some otehr examples of multiplicative groups:

- $\mathbb{Z}^\times = \{-1, 1\}$
- $M_n(R)^\times = GL_n(R)$ is called the *general linear group* (of $n \times n$ matrices over R).
- $(\mathbb{Z}/n\mathbb{Z})^\times = \{[a] : \gcd(a, n) = 1\}$ is a group with $\varphi(n)$ elements
- If $(A, +)$ is an abelian group, then $\mathrm{End}(A)^\times = \mathrm{Aut}(A)$

2 1/10/2024 lecture

A nonzero element a of a commutative ring R is called a *zero divisor* iff there exists a nonzero element b in R such that $ab = 0$.

2.1 Integral domains & subrings

If R is a nonzero commutative ring with no zero divisors, we call it an *integral domain* (or sometimes just *domain* for short). In an integral domain, multiplication by any nonzero element is an injection.

If R is finite, an injection from R to itself is also surjective and therefore invertible, so R is a field. However, not every integral domain is a field – for example, $\mathbb{Z}$ is a domain but not a field.

A subset S of a ring R is called a *subring* iff

- For any $a, b \in S$, $a + b, ab$, and $-a$ are also in S
- S contains 1, and $1_S = 1_R$.

If S is a subring of R, then $(S, +)$ is a subgroup of $(R, +)$.

$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ is a sequence of subrings.

The set of $n \times n$ matrices of the form

$$\begin{bmatrix} * & 0 \\ 0 & 0 \end{bmatrix}$$

is a ring and is also a subset of $M_2(\mathbb{R})$, but is not a subring of $M_2(\mathbb{R})$, because they do not have the same multiplicative identity element.

2.2 Ring homomorphisms

If R and S are rings, a map $f : R \to S$ is called a *ring homomorphism* iff

- $f(a + b) = f(a) + f(b)$ (that is, f is a group homomorphism)
- $f(ab) = f(a)f(b)$
- $f(1_R) = 1_S$

If S is a subring of R, then the inclusion map from S to R is a ring homomorphism.

A ring homomorphism is called a *ring isomorphism* iff it is bijective.

In **Ring** (the category of unital rings), $\mathbb{Z}$ is the initial object and 0 is the terminal object.

The map from $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ (for $n \in \mathbb{N}, n > 1$) which takes a to $[a]_n$ is a ring homomorphism.

One can show that there is no ring homomorphism from $\mathbb{Q}$ to $\mathbb{Z}$.

2.3 Ideals

If I is a subset of a ring R, we call I a *left ideal* iff

- I is closed under addition ($I + I \subset I$)
- For any $a \in I, x \in R$, xa is also in I (I is closed under left multiplication by any element of R, so $R \cdot I \subset I$)
- $I \neq \emptyset$ (we can use this to show that $0 \in I$)

The definition for a *right ideal* is the same, but with left multiplication replaced by right multiplication. A two-sided ideal is simply called an *ideal*.

Every ring has at least two ideals (itself, which is called the "unit ideal", and the zero ring), except for the zero ring (in which case the unit ideal is the zero ideal). If R is a field, those are the only ideals. Conversely, if R is a commutative ring whose only ideals are 0 and R, then R is a field. PROVE THIS.

For any $a \in R$, Ra is a left ideal and aR is a ring ideal. These are called the *principal left and right (respectively) ideals generated by a*.

In $M_n(\mathbb{R})$, the set of $n \times n$ real matrices with zeros everywhere except the first column is a left ideal.

If a left or right ideal I of R contains 1, then $I = R$. This is why we call I the "unit ideal". More generally, if I contains any invertible element (that is, $\exists u \in I \cap R^\times$), then $I = R$.

If I_α is a (possibly infinite) set of left (right) ideals, then $\cap_\alpha I_\alpha$ is a left (right) ideal. Also,

$$\sum_\alpha I_\alpha = \left\{ \sum_\alpha x_\alpha : x_\alpha \in I_\alpha, \text{ all except finitely many } x_\alpha \text{ are zero} \right\}$$

(the subgroup generated by I_α) is the smallest ideal containing all I_α.

For any elements $a_1, a_2, \ldots, a_n \in R$, we call $Ra_1 + Ra_2 + \cdots + Ra_n$ the *left ideal generated by* $a_1, \ldots, a_n$. Replacing Ra_i by a_iR, we get the *right ideal generated by the* a_i*s*.

For any ring homomorphism $f : R \to S$, the kernel of f is an ideal of R, and the image of f is a subring of S.

3 1/12/2024 lecture

3.1 Quotient rings

If $I \subset R$ is an ideal and $a, b \in R$, then we say that a and b are *congruent modulo* I ($a \equiv b \pmod{I}$) iff $b - a \in I$. If $a_1 \equiv b_1 \pmod{I}$ and $a_2 \equiv b_2 \pmod{I}$, then $a_1 + a_2 \equiv b_1 + b_2 \pmod{I}$ and $a_1 a_2 \equiv b_1 b_2 \pmod{I}$.

The set of cosets of I, $\{a + I \in R/I : a \in R\}$, is also a ring, called the *quotient ring* or the *factor ring*. $\mathbb{Z}/n\mathbb{Z}$ (for some natural number $n > 1$) is a classic example of a quotient ring.

For any ideal $I \subset R$, we can show that the canonical map $\pi : R \to R/I$ given by $\pi(a) = a + I$ is a surjective ring homomorphism, with $\operatorname{Ker}(\pi) = I$.

If $f : R \to S$ is a ring homomorphism, then we know that $\operatorname{Im}(f)$ is a subring of S and $\operatorname{Ker}(f)$ is an ideal of R. The *first isomorphism theorem for rings* says that the map $\overline{f} : R/\operatorname{Ker}(f) \to \operatorname{Im}(f)$ defined by $\overline{f}(a + \operatorname{Ker}(f)) = f(a)$ is not only a group homomorphism, but also a ring homomorphism.

Consider the function $f : \mathbb{R}[x] \to \mathbb{C}$ defined by $f(h) = h(i)$. This is a surjective ring homomorphism, and the kernel of f is the set of polynomials for which i is a root. Since f is real, it is invariant under complex conjugation, so a real polynomial h is in $\operatorname{Ker}(f)$ iff it is divisible by both $x - i$ and $x + i$. Therefore $\operatorname{Ker}(f) = (x^2 + 1)\mathbb{R}[x]$, so

$$\mathbb{R}[x]/((x^2 + 1)\mathbb{R}[x]) \cong \mathbb{C}.$$

3.2 Product of rings

An element e in any ring S is called *idempotent* iff $e^2 = e$. For example, 0 and 1 are idempotent in any ring.

For a ring R that is defined as the product of rings, $R := R_1 \times R_2 \times \cdots \times R_n$, the 0 element in R is $(0_{R_1}, \ldots, 0_{R_n})$, and similarly, $1_R = (1_{R_1}, \ldots, 1_{R_n})$. If $e_1 \in R_1, e_2 \in R_2, \ldots, e_n \in R_n$ are idempotents, the e_is are orthogonal (meaning $e_i e_j = 0$ when $i \neq j$), the e_is are all central ($e_i x = x e_i$ for any $x \in R$), and their sum is 1_R, then let the function $f : R \to Re_1 \times Re_2 \times \cdots \times Re_n$ be defined by $f(a) = (ae_1, \ldots, ae_n)$. We can prove that f is an isomorphism.

Fun example: the quotient ring $\mathbb{Z}/10^n\mathbb{Z}$ is isomorphic to $\mathbb{Z}/2^n\mathbb{Z} \times \mathbb{Z}/5^n\mathbb{Z}$. By Bézout's identity, $\mathbb{Z}/2^n\mathbb{Z} \times \mathbb{Z}/5^n\mathbb{Z}$ contains the elements $(0, 0)$, $(1, 0)$, $(0, 1)$, and $(1, 1)$, which are all idempotent – in fact, these are the only idempotent elements. Since that group is isomorphic to $\mathbb{Z}/10^n\mathbb{Z}$, we know that for any n, there are exactly 4 integers between 1 and 10^n whose square has the last same n digits as the original number. Those are precisely the 4 numbers which are congruent to either 0 or 1 in both $\mathbb{Z}/2^n\mathbb{Z}$ and $\mathbb{Z}/5^n\mathbb{Z}$. Two of those numbers are boring (zero and one), but the other cases are interesting.

4 1/17/2024 lecture

Let I and J be ideals of R. We say that they are *coprime* iff $I + J = R$. For example, integers n and m are relatively prime if and only if $n\mathbb{Z}$ and $m\mathbb{Z}$ are coprime.

4.1 Chinese remainder theorem

The *Chinese Remainder Theorem (CRT)* says that if $I_1, I_2, \ldots, I_n$ are pairwise coprime ideals of a ring R, then for every tuple $(a_1, \ldots, a_n) \in R^n$, there exists $a \in R$ such that $a \equiv a_j \pmod{I_j}$ for every index j. We prove this by induction on $n \geq 2$.

If $n = 2$, then for any $a_1, a_2 \in R$, since $I_1 + I_2 = R$ and $a_1 - a_2$ is in R, there must be some $x_1 \in I_1, x_2 \in I_2$ such that $x_1 + x_2 = a_1 - a_2$. Then it is easy to show that $a - a_j \in I_j$, which implies $a \equiv a_j \pmod{I_j}$ (for either $j = 1$ or $j = 1$).

If the CRT is true for some $n-1$, then $I_1 \cap I_2 \cap \cdots \cap I_{n-1}$ and I_n are coprime, so we can use the same method that we used to prove it works when $n = 2$ to show that (if it works for $n-1$) it also works for n, so by induction, it works for any $n \geq 2$.

An equivalent statement to CRT is that if $I_1, I_2, \ldots, I_n$ are pairwise coprime ideals of a ring R, then the function

$$f : R \to (R/I_1) \times (R/I_2) \times \cdots \times (R/I_n)$$

defined by

$$a \mapsto (a + I_1, a + I_2, \ldots, a + I_n)$$

is surjective. If that function f is surjective, then $\mathrm{Ker}(f) = I_1 \cap I_2 \cap \cdots \cap I_n$, which implies

$$R/(I_1 \cap \cdots \cap I_n) \cong (R/I_1) \times \cdots \times (R/I_n).$$

4.2 Prime ideals

Let R be a commutative ring. An ideal $P \subsetneq R$ is called *prime* iff $ab \in P$ implies $a \in P$ or $b \in P$ (for any $a, b \in R$).

An ideal $P \subsetneq R$ is prime if and only if R/P is a domain. NEED TO PROVE THIS.

Example: the following statements are all equivalent:

- $n\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$
- $\mathbb{Z}/n\mathbb{Z}$ is a domain
- n is either prime or zero

4.3 Maximal ideals

Let R be a commutative ring. An ideal $M \subsetneq R$ is called *maximal* iff there is no ideal between M and R (that is, there is no ideal I such that M is a proper subset of I and I is a proper subset of R).

An ideal $M \subsetneq R$ is maximal if and only if R/M is a field. Proof: STILL NEED TO WRITE THIS PROOF.

Every maximal ideal is prime.

4.4 Posets and chains

Let X be a set with a relation denoted by $\preceq$. We call X a *partially-ordered set (poset)* iff for any $x, y, z \in X$,

- $x \preceq x$
- If $x \preceq y$ and $y \preceq x$, then $x = y$
- If $x \preceq y$ and $y \preceq z$, then $x \preceq z$

A *chain* in a poset X is a subset $S \subset X$ such that for any $x, y \in S$, $x \preceq y$ or $y \preceq x$ (equivalently, S is *totally ordered*).

An element $x \in X$ is called an *upper bound* of a chain S iff $s \preceq x$ for every $s \in S$. A *maximal element* of X is any element $x \in X$ such that if $x \preceq y$, then $x = y$.

Zorn's lemma states that if X is a nonempty poset such that every chain in X has an upper bound in X, then X has a maximal element (possibly multiple). This statement is logically equivalent to the axiom of choice, which we assume to be true for the purpose of this class.

We can use this to prove that every nonzero commutative ring R has a maximal ideal (if every chain of non-unit ideals of R has an upper bound). Proof: Define an order relation on the set X of all ideals $I \subsetneq R$ (excluding the zero ideal) by saying $I \preceq J$ if and only if $I \subset J$. Then X has at least one maximal element, which is a maximal ideal of R.

Simple corollary of that: every nonzero commutative ring has a prime ideal.

5 1/19/2024 lecture

5.1 Field of fractions

Let R be a domain. Then let $\mathcal{F}(R)$ be the *field of fractions over* R, defined as the quotient of

$$\{(a, b) : a, b \in R, b \neq 0\}$$

by the equivalence relation that $(a, b) \sim (a', b')$ iff $a'b = ab'$. We can easily prove that the operations in $\mathcal{F}(R)$ are well-defined (addition and multiplication are defined exactly how you expect), and that the notation you would expect you can use for fractions is indeed valid here.

If R is a subring of a field K such that every $x \in K$ can be written as $x = ab^{-1}$, for some $a, b \in R, b \neq 0$. Then K is isomorphic to $\mathcal{F}(R)$. Proof: we can show that the mapping from x to $\frac{a}{b}$ is a ring isomorphism, taking advantage of the fact that every ring homomorphism from a field to a nonzero ring is injective (WHY IS THIS TRUE???).

5.2 Euclidean rings

A *Euclidean ring* is a domain R such that there exists a function $\varphi : R \setminus \{0\} \to \mathbb{Z}^{\geq 0}$ satisfying the following property: for any $a, b \in R, b \neq 0$, there exist $q, r \in R$ such that $a = bq + r$ and either $\varphi(r) < \varphi(b)$ or $r = 0$.

Examples:

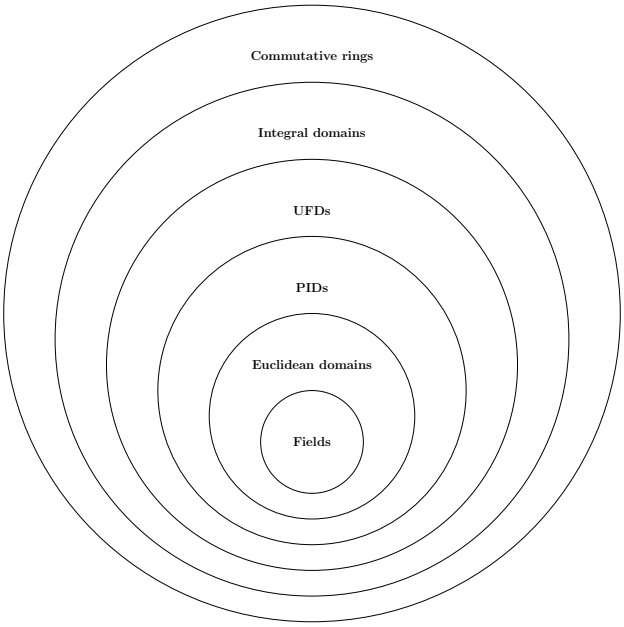
- $\mathbb{Z}$ is a Euclidean domain because we can define a Euclidean function $\varphi(a) = |a|$.
- If $\mathbb{F}$ is a field, then $R = \mathbb{F}[x]$ is a Euclidean domain because we can define $\varphi(f) = \deg(f)$.
- The *Gauss integers*, $R = \mathbb{Z}[i] \subset \mathbb{C}$, are a Euclidean domain because we can define $\varphi(a+bi) = a^2 + b^2$. Proving that this works is kind of a pain, but you can use a super similar method to show some domains like $\mathbb{Z}[\sqrt{2}]$ are also Euclidean.

6 1/22/2024 lecture

A domain R is called a *principal ideal domain (PID)* iff every ideal in R is principal.

Every Euclidean domain is a PID. Proof: Let I be an ideal of R, and assume $I \neq 0$. There exists a Euclidean function $\varphi : R - \{0\} \to \mathbb{Z}^{\geq 0}$. Let $a \in I$ be a value of $I - \{0\}$ which minimizes $\varphi(a)$. Now suppose $I = aR$. Since I is PID, we know $aR \subset I$, so for every $x \in I$, there exist $q, r \in R$ such that $x = aq + r$ and either $r = 0$ or $\varphi(r) < \varphi(a)$. If $r \neq 0$, then $= aq \in I$, so r is a nonzero element of I such that $\varphi(r) < \varphi(a)$. This is a contradiction, so every Euclidean domain is a PID. REDO THIS PROOF BECAUSE IT IS A HUGE MESS.

$\mathbb{Z}$ and $\mathbb{F}[x]$ (for some field $\mathbb{F}$) and $\mathbb{Z}[i]$ are examples of PIDs.



TODO: move that figure to the point in the notes where we prove which of those are subsets of which others

6.1 Factorization in integral domains

Let a, b be elements of a domain R such that $b \neq 0$. We say that b *divides* a (written $b|a$) iff $a = bc$ for some $c \in R$. This is equivalent to saying $aR \subset bR$. a and b are called *associate*

iff $a|b$ and $b|a$ (in other words, $aR = bR$). Sometimes we write $a \sim b$ to denote that a and b are associate, because being associate is an equivalence relation.

This is an example of a "good" property". A *good property* is any property that can be written in terms of ideals.

If a and b are associate elements of a domain R, then $a = bc$ for some $c \in R$, and $b = ad$ for some $d \in R$. Then $a = adc$, so $dc = 1$. This means there exists a unit $u \in R^\times$ (either $u = c$ or $u = d$) such that $a = bu$ and $b = au^{-1}$.

Also, note that multiplying any two elements a, b by a unit does not change whether one divides the other.

6.2 Irreducible elements

An element c of a domain R is called *irreducible* iff $c \neq 0$, $c \notin R^\times$, and any $a, b \in R$ such that $c = ab$, either $a \in R^\times$ or $b \in R^\times$.

Equivalently, an element $c \in R$ is irreducible iff cR is maximal in the set of principal ideals which are not R. Proof: suppose there exists $a \in R$ such that $cR \subsetneq aR \neq R$. Then a is not invertible, and since $c \in cR$, we can write $c = ab$, which implies b is invertible. This is a contradiction, because we could write $cR = abR$, and since b is invertible, that implies $cR = aR$. REMEMBER TO ADD THE PROOF GOING THE OTHER WAY, SINCE THE STATEMENT WAS "IF AND ONLY IF".

6.3 Prime elements

An element $p \in R$ is called *prime* iff $p \neq 0$, $p \notin R^\times$, and if $p|ab$, then either $p|a$ or $p|b$.

Now we want to make this a good property. An element inR is prime if and only if $p \neq 0$ and pR is a prime ideal. Proof: the definition of a prime element can be rewritten as "for any elements $a, b \in R$, if $ab \in pR$, then $a \in pR$ or $b \in pR$".

Every prime element is irreducible (but the converse is not true). Proof: Let p be a prime element of R such that $p = ab$. Then without loss of generality, we can say p divides a, so let c be the element such that $a = pc$. This implies $p = pcb$, so b is invertible.

Example: let $R = \mathbb{Z}[\sqrt{-5}] \subset \mathbb{C}$. Since $2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ but 2 does not divide $1 \pm \sqrt{-5}$, 2 is not prime in R. However, we can show that 2 is irreducible in R (TODO: ADD PROOF OF THAT).

7 1/24/2024 lecture

REDO ALL NOTES FROM THIS LECTURE.

In a PID, every irreducible element is prime. Proof: Suppose c is an irreducible element of a PID R. Then cR is maximal in the set of all principal ideals, but R is a PID, so cR is a maximal ideal, therefore it's a prime ideal, so c is prime.

If I, J are ideals in a commutative ring R, define

$$I \cdot J = \left\{ \sum x_i, y_i : x_i \in I, y_i \in J \right\}.$$

This is clearly an ideal. The simplest such example is $(aR) \cdot (bR) = abR$.

If R is a domain containing some nonzero, noninvertible element a, then $a = c_1c_2\cdots c_n$ (WHY DO WE ASSUME THIS IS FINITE???) for c_i irreducible in R. Conversely, if $aR = (c_1R)(c_2R)\cdots(c_nR)$, then we can multiply both sides by a unit to see that a is the product of irreducible elements. FIX UP THE LAST PART OF THIS DEFINITION.

In general, we say that R has a *unique factorization* iff whenever $a = c_1c_2\cdots c_n = d_1d_2\cdots d_m$ (where every c_i and c_j is irreducible), $n = m$ and there exists a permutation $\sigma \in S_n$ and a set of units $u_i \in R^\times$ such that $c_i = u_i d_{\sigma(i)}$ for every index i.

Let R be a domain, and suppose that R *admits factorization* (meaning every element can be written as a product of primes). If the factorization is unique, then every irreducible element is prime, and if every irreducible element is prime, then the factorization is unique. Proof: Let $c \in R$ be an irreductible element, and suppose there exist $a, b \in R$ such that $c|ab$. Let $x_1x_2\cdots x_n = a$ and $y_1, y_2\cdots y_m = b$ be unique factorizations of a and b. Since c and divides ab, there is an element d such that $ab = cd$, and we can let $z_1z_2\cdots z_k$ be a unique factorization of d. Then we have

$$\prod x_i \prod y_j = c \prod z_l$$

which means c divides either some x_i or some y_j, so c divides either a or b. Proof going the other direction: Let $a = c_1c_2\cdots c_n = d_1d_2\cdots d_m$ be two factorizations of a where each c_i, d_j is irreducible (and therefore prime).

7.1 Nifty trick

If $(xR)(cR) = (yR)(cR)$, then $xcR = ycR$, so $xc = ycu$ for some $u \in R^timesi$. Somehow we cancel the c out (WHAT PROPERTY OF c ARE WE USING TO DO THIS???) and we get that $xR = yR$.

7.2 Unique factorization domains

A domain R is a *unique factorization domain (UFD)* iff R admits factorization and the factorization is unique. As we just proved, every irreducible element in a UFD is prime – equivalently, a domain is a UFD iff it admits factorizatin and every irreducible element in that domain is prime.

We will prove later on that every PID generated by finitely many elements is a UFD. A ring generated by finitely many elements is called a *Noetherian ring*.

8 1/26/2024 lecture

8.1 Noetherian rings

Let R be a commutative ring. Then the following are equivalent:

- Every ideal in R is finitely generated (meaning there is a finite set of elements $a_1, \ldots, a_n$ such that $I = a_1R + a_2R + \cdots + a_nR$)

- Every chain of ideals terminates, meaning if there is a sequence of ideals $I_1 \subset I_2 \subset I_3 \subset \cdots$, then there exists N such that for any $N' \geq N$, $I_N \subset I_{N'}$
- Every nonempty set of ideals of R has a maximal element

We call R *Noetherian* iff it satisfies those properties.

Every PID is Noetherian.

The *Hilbert basis theorem* states that if R is a Noetherian ring, then so is $R[x]$. We can extend this by induction to show that if R is Noetherian, then the set of polynomials in finitely many variables ($R[X_1, x_2, \ldots, X_n]$) is Noetherian as well.

Every Noetherian domain admits factorization. Proof: let A be the set of principal ideals aR which do not admit factorization, and suppose A is nonempty. Then let aR be a maximal element of A. Since a is not irreducible, there exist noninvertible elements $b, c \in R \backslash R^\times$ such that $a = bc$ FINISH TYPING UP THIS PROOF

Example: the ring $R = \mathbb{Z}[i]$ contains the element 2 which is the product of irreducible elements $1+i$ and $1-i$, so $2 = i \cdot (1-i)^2$, which implies $2R = ((1-i)R)^2$. Therefore $2R$ can be factored (which we know is true because $2R$ is a PID). WHAT WAS THIS SUPPOSED TO BE AN EXAMPLE OF?

9 1/29/2024 lecture

Let R be a Noertherian domain. Then it is a UFD if and only if every irreducible is prime (that is, if it admits factorization)

The GCD of a and b in a ring R is the element c such that cR is a subset of aR and of bR and the cR is minimal

10 1/31/2024 lecture

11 2/5/2024 lecture

If R is a UFD, then so is $R[x]$. We are especially interested in the case where R is a field.

11.1 Factorization of polynomials over fields

Let $\mathbb{F}$ be a field and let $f \in \mathbb{F}[x]$. Then $a \in \mathbb{F}$ is a *root* of f if and only if $f(a) = 0$. Proposition: a is a root of f if and only if f is divisible by $x - a$ in $\mathbb{F}[x]$. Proof: since $\mathbb{F}[x]$ is a Euclidean domain, there exist polynomials g and r such that $f = (x-a) \cdot g + r$, where r is degree 0 and the degree of g is at most $\deg(f) - 1$. If $r = 0$, then $f(a) = g(a)(a-a) = 0$, and if $r \neq 0$, then $f(a) = r(a) \neq 0$.

If $f = (x-a_1)(x-a_2)\cdots(x-a_m)\ell$, where $\ell \in \mathbb{F}[x]$ has no roots, then the roots of f are $\{a_1, a_2, \ldots, a_m\}$. Corollary: a nonzero $f \in \mathbb{F}[x]$ has at most $\deg(f)$ roots in $\mathbb{F}$.

Formally, the ring of polynomials $R[x]$ is a sequence of coefficients in R, but we also interpret a polynomial in $R[x]$ as a function from R to R. However, this doesn't always work

– in $\mathbb{Z}/2\mathbb{Z}$, for example, the polynomials x and x^2 (and any $x^n, n \in \mathbb{N}$) would be the same function, because they are both the identity map on $\mathbb{Z}/2\mathbb{Z}$.

However, if $\mathbb{F}$ is an infinite field and $f, g \in \mathbb{F}[x]$ and $f(a) = g(a)$ for every $a \in \mathbb{F}$, then $f = g$. Proof: If $f(a) - g(a) = (f - g)(a) = 0$, then $f - g$ is a polynomial with infinitely many roots, so it must be zero.

If $\deg(f) = 1$, then f can be written as $ax + b$. Assuming $a \neq 0$, f has exactly one root, which is $-b/a$, and f is irreducible. If $\deg(f) > 1$ and f has a root a, then f is reducible. Corollary: any degree 2 or 3 polynomial which is reducible must have a root, but this does not work for degree 4, because the polynomial $(x^2 + 1)(x^2 + 2) \in \mathbb{R}[x]$ is reducible but does not have any roots.

11.2 Eisenstein's criterion

Eisenstein's criterion: Let R be a UFD, and let $\mathbb{F}$ be the field of fractions of R. Let $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in R[x]$. Assume that for some prime $p \in R$ (since R is a UFD, p is irreducible), we have

- $p \nmid a_n$ (p does not divide a_n)
- $p | a_i$ for all $i < n$
- $p^2 \nmid a_0$

If f satisfies all those criteria, then f is irreducible in $\mathbb{F}[x]$. Proof: Suppose f satisfies all those criteria but is reducible. Then there exist lower degree polynomials $g, h \in \mathbb{F}[x]$ such that $= g \cdot h$. For some unit $\alpha \in \mathbb{F}^\times$, αg is primitive in $R[x]$, so without loss of generality, we can assume g is primitive in $R[x]$ (by replacing g with αg and h with $\alpha^{-1} h$). Since $g | f$ in $\mathbb{F}[x]$, $g | f$ in $R[x]$ as well, so $h \in R[x]$. Now define the domain $\overline{R} = R/pR$, and let $\overline{a}$ be the value which the induced map takes $a \in R$ to. Similarly, there is an induced map which takes any $f \in R[x]$ to $\overline{f} \in \overline{R}[x]$. Since $\overline{f} = \overline{a_n} x^n \neq 0$, FINISH PROOF OF THAT!!! ALSO, WHAT DOES PRIMITIVE MEAN???

Example 1: $x^4 - 12 \in \mathbb{Q}[x]$ is irreducible, because we can apply the Eisenstein criteria with $R = \mathbb{Z}$ and $p = 3$.

Example 2: If K is a field, then the polynomial $xy^3 + y^3 - xy^2 + x \in K[x, y]$ is irreducible. COPY PROOF OF THIS FROM SOMEONE ELSE'S NOTES.

12 2/7/2024 lecture

modules?? classic examples are vector spaces over a field and abelian groups over Z

13 2/9/2024 lecture

13.1 R-module homomorphisms

If R is a ring and M is an abelian group, then there is a bijection from the set of left R-modules structures on M and $\mathrm{Hom}_{\mathrm{ring}}(R, \mathrm{End}(M))$, which maps r to a function f defined

by $f(r)(m) = r \cdot m$. WHAT WAS THE THINGY WE MENTIONED ABOUT PULLBACKS?? Similarly, we can define a bijection from the set of right R-module structures and $\mathrm{Hom}(R^{\mathrm{op}}, \mathrm{End}(M))$.

Let R be a ring, and let M, N be left R-modules. A *homomorphism of R-modules* is a map $f : M \to N$ such that f is a homomorphism of abelian groups and $f(am) = af(m)$ for any $a \in R, m \in M$.

There is always at least one R-module homomorphism from any M to any N – namely, the zero morphism.

We can add any two R-module homomorphisms from M to N, so the set of those morphisms forms an abelian group, which we denote by

$$\mathrm{Hom}_R(M, N).$$

If R is a field, then any module over R is a vector space, so R-module homomorphisms are simply linear maps of vector spaces.

If $R = \mathbb{Z}$, then $\mathbb{Z}$-module homomorphisms are abelian group homomorphisms.

An R-module homomorphism $f : M \to N$ is an isomorphism iff f is a bijection. Equivalently, this means f is an isomorphism of abelian groups. If f is an isomorphism, then $f^{-1} : N \to M$ is also an R-module isomorphism.

13.2 Submodules

If N is a subset of a (left) R-module M, we call N a *submodule (of M)* iff N is a subgroup of M and $an \in N \forall a \in R, n \in N$. A submodule of M is always a (left) R-module.

If R is a field, then submodules are vector subspaces. If $R = \mathbb{Z}$, then submodules are subgroups.

A (left) ideal $I \subset R$ is a submodule.

If $f : M \to N$ is a (left) R-module homomorphism, then $\mathrm{Ker}(f) \subset M$ and $\mathrm{Im}(f) \subset N$ are submodules.

If $(N_i)_{i \in I}$ is a family of submodules of a (left) R-module M, then $\cap_{i \in I} N_i$ is alse a submodule of M. The sum of a family of submodules is defined as

$$\sum_{i \in I} = \left\{ \sum_{i \in I} n_i : n_i \in N_i, \text{ all but finitely many } n_i \text{ are zero} \right\}.$$

Sometimes we say "almost all" instead of "all but finitely many". That sum is the smallest submodule of M that contains all N_i, and similarly, the intersection of every N_i is the largest submodule contained in every N_i.

13.3 Quotient modules

If N is a submodule of a (left) R-module, then M/N is an abelian group. With addition defined by $a \cdot (m + N) = am + N$. Of course, we need to check that this is well-defined. In fact, M/N turns out to be a (left) R-module, which we call the *quotient module* or *factor module*. The map $\pi : M \to M/N$ defined by $m \mapsto m + N$ is called the *canonical R-module homomorphism*, and its kernel is N.

We now have a whole bunch more isomorphism theorems:

- **First isomorphism theorem:** If $f : M \to N$ is an R-module homomorphism, then the map $\overline{f} : M/\operatorname{Ker}(f) \to \operatorname{Im}(f)$ defined by $\overline{f}(m + \operatorname{Ker}(f)) = f(m)$ and $\overline{f}(a(m + \operatorname{Ker}(f))) = \overline{f}(am + \operatorname{Ker}(f))$ is an R-module isomorphism. REWRITE THIS MORE SIMPLY AND ALSO APPLY IT TO PROVE RANK NULLITY THEOREM

- **Second isomorphism theorem:** If $N, P \subset M$ are two submodules, then there is a module isomorphism from $P/(N \cap P)$ to $(N + P)/N$ defined by $p + (N \cap P) \mapsto p + N$.

- **Third isomorphism theorem:** If $N \subset P \subset M$ are submodules, then $(N/N)/(P/N) \cong M/P$.

13.4 Product modules

If $M_1, M_2, \ldots, M_n$ are (left) R-modules, then the *external direct sum* of them is $M_1 \oplus M_2 \oplus \cdots \oplus M_n$.

If $N_1, N_2, \ldots N_n \subset M$ are submodules, then we say that M is the *internal direct sum* iff every $m \in M$ can be uniquely written as $m = x_1 + x_2 + \cdots x_n$, where $x_i \in N_i$. Then there is a bijection from $N_1 \oplus N_2 \oplus \cdots \oplus N_n$ to M which maps $(x_1, x_2, \ldots, x_n)$ to $\sum_{i=1}^{n} x_n$, so this is an R-module isomorphism.

14 2/12/2024 lecture

15 2/14/2024 lecture

15.1 Modules over a PID

If R is a domain and $N \subset R^n$ is a submodule, we want to know whether N is free. If $n = 1$, then since R is free and every submodule of a free module is free, N is free, and N is principal, so R is a PID.

Theorem: Let R be a PID. Then every submodule of R^n is free of rank $\leq n$.

Proof. If $n = 1$, then as shown above, any $N \subset R^n$ is a principal ideal, so N is free. Suppose every submodule of R^{n-1} is free of rank $\leq n - 1$. Then for any $N \subset R^{n-1}$, let $f : N \to R$ be the function that maps $(a_1, a_2, \ldots, a_n)$ to a_n. The kernel of f is a subset of R^{n-1}, so $\operatorname{Ker}(f)$ is free of rank $\leq n - 1$. The image of f is an ideal of R, and since that ideal is principal (WHYYY???), there is some $c \in R$ such that $\operatorname{Im}(f) = cR$. If $c = 0$, then $N = \operatorname{Ker}(f)$, which is free of rank $\leq n - 1$, so we're done. If $c \neq 0$, let $y \in N$ be an element such that $f(y) = c$. Then we can choose a basis $(x_1, \ldots, x_k)$ for $\operatorname{Ker}(f) \subset R^{n-1}$ (where $k \leq n - 1$), so then $(x_1, x_2, \ldots, x_k, y)$ is a basis for N.

For any $x \in N$, $f(x) \in \operatorname{Im}(f) = cR$, so there exists some $d \in R$ such that $f(x) = cd$. Now let $x' = x - dy$. so $f(x') = f(x) - df(y) = cd - dc = 0$. Since $x' \in \operatorname{Ker}(f)$, there exist $a_i \in R$ such that $a_1x_1 + \cdots + a_kx_k = x'$, which implies $x = a_1x_1 + a_2x_2 + \cdots + a_kx_k + dy$. If $f(x) = 0$, then FINISH THIS PROOF TO SHOW THAT THE COEFFICIENTS OF THE BASIS ELEMENTS ARE ZERO. □

Corollary: Let R be a PID, M an R-module generated by n elements. Then every submodule of M is generated by $\leq n$ elements.

Proof of that corollary: There is a surjective (R-module) homomorphism f from R^n to M. For any submodule P of M, let $N = f^{-1}(P)$. Then N is a submodule of R^n generated by $\leq n$ elements, and since the restriction of f to N (which we will call $g : N \to R^n$) is also a surjective R-module homomorphism, that means P is also generated by $\leq n$ elements.

If we let $m \leq n$ be the rank of $N = \mathrm{Ker}(f)$, then $\mathrm{Im}(g) = N$. By the first isomorphism theorem, $M \cong R^n/N = R^n/\mathrm{Im}(g)$.

Note: in this class, we assume all R-modules are finitely generated.

A *presentation* of an R-module M is a homomorphism $g : R^m \to R^n$ together with an isomorphism from M to $R^n/\mathrm{Im}(g)$. There is an $n \times m$ matrix A such that $g(x) = A \cdot x$.

15.2 Matrix transformations

Suppose A is an $N \times M$ matrix over R. For now, we will assume R is a Euclidean domain, such as $R = \mathbb{Z}$ or $R = \mathbb{F}[x]$. Consider the following transformations:

- Swap two rows (or columns)
- Add a multiple of a row (or column) to another row (or column) WHAT DOES IT MEAN TO TAKE A MULTIPLE OF AN ELEMENT OF A RING???
- Multiply a row (or column) by a unit $u \in R^\times$.

A matrix A has *normal form* iff everything off the main diagonal is zero, and the elements in the main diagonal form the sequence $(d_1, d_2, \ldots, d_k, 0, \ldots, 0)$, where $d_i \neq 0$ and $d_1 | d_2 | \cdots | d_k$. Getting a matrix over a ring into normal form is harder than standard Gaussian elimination, because we can't assume every element of R has an inverse.

Proposition 15.1.

Proposition: If R is a Euclidean domain, then every matrix over R can be converted to normal form by using the 3 matrix transformations. Proof: let $\varphi : R \setminus \{0\} \to \mathbb{Z}^{\geq 0}$ be a Euclidean function and let A be a nonzero $m \times n$ matrix over R. Let $a \in R$ be a nonzero element such that $\varphi(a)$ is minimized (HOW DO WE KNOW A MINIMUM EXISTS???), where a is an entry of a matrix that can be obtained from A using any of the 3 matrix transformations. FINISH THE REST OF THIS PROOF, EVEN THOUGH IT IS KINDA LONG – we can define an algorithm to get everything in the top row xor in the leftmost olumn to be zero, and everything else in the matrix to be to divisible by the top left element, then use induction on matrix size. NOTE THAT THE ZERO MATRIX IS ALREADY IN NORMAL FORM

16 2/16/2024 lecture

The proof we did last lecture was a bit janky, because we did not rigorously define the algorithm for getting a matrix into normal form. I'm not gonna write out the whole algorithm

though, because it's long and boring. Here's the quick version: if R is a Euclidean domain and $A \in R^{m\times n}$, then we can use the 3 row operations (or instead, we could use only column operations) in a way that sort of resembles the Euclidean algorithm.

Any such matrix A, when written in normal form, will have the sequence $(d_1, d_2, d_3, \ldots, d_k, 0, 0, \ldots, 0)$ along the diagonal and zero everywhere else, where $d_i | d_{i+1}$ and $k \leq \min(n, m)$. Note that all of the units are at the beginning of that sequence – that is, $d_i \in R^\times, i > 1$ implies $d_{i-1} \in R^\times$.

Applying any of the 3 elementary row operations is equivalent to left-multiplying by some invertible $m \times m$ matrix over R. Similarly, any column operation is equivalent to right-multiplication by some invertible $n \times n$ matrix over R. These matrices look exactly like the ones we've learned in lower-div linear algebra, except that the entries are elements of R instead of $\mathbb{R}$, and the matrix which multiplies a row (or column) by a unit must have units on the diagonal (all but one of which are 1).

Proposition 16.1. *Let $A \in M_{m,n}(R)$, where R is a Euclidean domain. Then there exist $B \in GL_m(R)$ and $C \in GL_n(R)$ such that BAC has normal form.*

Let $f : R^n \to R^m$, $g : R^m \to R^m$, and $h : R^n \to R^n$ be the ring homomorphisms defined as left multiplication by A, B, and C, respectively. If M is a finitely generated R-module defined as $R^m / \operatorname{Im}(f)$ (DID PROF ALSO CLAIM THAT FOR ANY FINITELY GENERATED M, WE CAN CHOOSE A SUCH THAT $M \cong R^m / \operatorname{Im}(f)$???), then $N = R^m / \operatorname{Im}(gfh)$ is isomorphic to M.

Proof. Use the first isomorphism theorem and a little bit of diagram chasing. □

This means the image of gfh is the column space of BAC. More precisely,

$$\operatorname{Im}(gfh) = d_1R \oplus d_2R \oplus \cdots \oplus d_kR \oplus 0 \oplus 0 \oplus \cdots \oplus 0 \in R^n$$

which implies

$$M \cong R^n / \operatorname{Im}(gfh) = (R/d_1R) \oplus (R/d_2R) \oplus \cdots \oplus (R/d_kR) \oplus R \oplus R \oplus \cdots \oplus R.$$

Theorem 16.2. *Let M be a finitely generated module over a PID R. Then there exists $d_1 | d_2 | \cdots | d_r$ such that $d_i \neq 0, d_i \notin R^\times$ and*

$$M \cong (R/d_1R) \oplus \cdots \oplus (R/d_rR) \oplus R^s$$

for some $s \geq 0$.

Proof. We will prove this later, and also show that this sequence of d_i is unique. The general idea for making it unique is to find a normal-form matrix A such that M is the quotient of R^m by the column space of f, and we canignore any of the diagonal entries in A which are units. The elements $(d_1R, d_2R, \ldots, d_rR)$ are called *invariant factors of M*, and are denoted by $IF(M)$. □

17 2/21/2024 lecture

See notes from Bockman

18 2/23/2024 lecture

18.1 Prime ideals

Let P be a nonzero prime ideal of a PID R. Then there exists a prime element $p \in R$ such that $P = pR$. If M is a finitely generated R-module, then $M/pM = M/PM$ is a finite dimensional vector space over $K_p = R/P$ (recall that the quotient of a commutative ring by a maximal ideal is always a field, called the *residue field*).

By the same reasoning, $p^i M/p^{i+1}M$ is also a (finite dimensional) vector space over K_p, and we can define the following function, which we use throughout this lecture:

$$f_i(M) = \dim_{K_p} \left(p^i M/p^{i+1}M\right).$$

If $i \geq n$ then $f_i(R/p^n R) = 0$.

If $i < n$ then the third isomorphism theorem says that $p^i M/p^{i+1}M \cong p^i R/p^{i+1}R$, so there exists a surjective ring homomorphism that takes $a \in R$ to $p^i a + p^{i+1}R \in p^i R/p^{i+1}R$. By looking at the kernel of that map and then applying the first isomorphism theorem, we get $K_p \cong p^i R/p^{i+1}R$ so $f_i(M) = 1$.

If Q is a prime ideal of R, and Q is not the same as the prime ideal $P \subset R$, then we want to find $R/Q^n R$. P^i and Q^n are relatively prime, so we can show that $p^i M \cong M$, which means that $f_i(R/Q^n) = 0$ whenever Q and P are distinct prime ideals (note that the definition of f_i depends on P).

18.2 Torsion modules

Let the R-module M be the direct sum of M_{tors} (which itself is the direct sum of primary cyclic R-modules) and the free module R^s. Then M_{tors} is the direct sum of cyclic modules which all have the form $R/p^n R$, where p is some prime element of R. Using the property we proved above about calculating $f_i(R/Q^n) = 0$ when Q and P are coprime, we can fix p, and then for the purpose of calculating f_i, we can ignore all terms which don't have the form $R/p^n R$ (for the fixed p).

$$\begin{aligned}
M_{\text{tors}} &= (R/pR)^{\oplus a_1} \oplus (R/p^2R)^{\oplus a_2} \oplus \cdots \oplus (R/p^t R)^{\oplus a_t} \oplus (\text{other terms}) \\
f_i(M_{\text{tors}}) &= a_{i+1} + a_{i+2} + \cdots + a_t \\
f_{i-1}(M_{\text{tors}}) &= a_i + a_{i+1} + \cdots + a_t \\
a_i &= f_{i-1}(M_{\text{tors}}) - f_i(M_{\text{tors}})
\end{aligned}$$

This shows that invariant factors are unique and elmentary divisors are unique up to permutation, so for finitely generated R-modules N, M,

$$N \cong M \iff \text{IF}(N) = \text{IF}(M) \iff \text{ED}(N) = \text{ED}(M).$$

18.3 Abelian groups are modules

A finitely generated R-module can be presented as $M \cong R^n/N$. Let $x_1, x_2, \ldots, x_n$ generate $N \subset R^n$ and let A be an $n \times m$ matrix whose columns are $x_1, x_2, \ldots, x_n$. Left multiplication

by A is a ring homomorphism $f : R^m \to R^n$ with $\mathrm{Im}(f) = N$, which means $M \cong R^n/\mathrm{Im}(f)$. If you put A in normal form, the image of f doesn't change, so

$$M \cong (R/d_1R) \oplus (R/d_2R) \oplus \cdots \oplus (R/d_rR) \oplus R^s$$

where the invariant factors of M are

$$\mathrm{IF}(M) = \{d_1R, d_2R, \cdots, d_rR\}.$$

I THINK I MISINTERPRETED THIS LAST PART BECAUSE I DONT SEE HOW THE GENERATORS X ARE RELATED TO THE INVARIANT FACTORS D.

Corollary 18.1. *Let M be a finitely generated torsion R-module. Then M is cyclic if and only if $|\mathrm{IF}(M)| = 1$.*

Proof. TODO: DO THIS PROOF, IT SHOULD BE FAIRLY EASY □

Every $\mathbb{Z}$-module is an abelian group, and vice versa. Also, primary cyclic $\mathbb{Z}$-modules have the form $\mathbb{Z}/p^n\mathbb{Z}$.

Theorem 18.2. *Every finitely generated abelian group is isomorphic to*

$$\mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_r\mathbb{Z} \oplus \mathbb{Z}^s$$

for unique positive integers s and $d_1|d_2|\cdots|d_r$.

Proof. Use the fact that abelian groups are $\mathbb{Z}$-modules. □

Theorem 18.3. *Every finitely generated abelian group is isomorphic to*

$$\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \oplus \mathbb{Z}/p_2^{\alpha_2}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_t^{\alpha_t}\mathbb{Z} \oplus \mathbb{Z}^s$$

for unique (up to permutation) prime powers $p_1^{\alpha_1}, \ldots, p_t^{\alpha_t}$ and unique $s \geq 0$.

Proof. TBH I DONT REMEMBER THE PROOF BUT ITS THE SPECIAL CASE FOR R=Z OF SOMETHING WE DID EARLIER □

If A is a finitely generated abelian group, then for some $n > 0$, we can define $A[n]$ to be $\{a \in A : na = 0\}$.

Lemma 18.4. *If $|A[n]| \leq n$ for every $n \geq 0$, then A is cyclic.*

Proof. If there are two invariant factors $d_1|d_2$, then $A[d_1] \geq d_1^2 > d_1$. If there is only one invariant factor, then STILL NEED TO FINISH THIS PROOF. □

19 2/26/2024 lecture

19.1 Cyclic modules

Theorem 19.1. *Let $\mathbb{F}$ be a field and $A \subset \mathbb{F}^\times$ a finite subgroup. Then A is cyclic.*

Proof. It suffices to show that $|A[n]| \leq n$ for any $n > 0$. Since

$$A[n] = \left\{a \in \mathbb{F}^\times : a^n = 0\right\},$$

the elements of $A[n]$ are precisely the roots of $x^n - 1$. □

Corollary 19.2. *If $\mathbb{F}$ is a finite field, then $\mathbb{F}^\times$ is cyclic. In particular, $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic for any prime p.*

19.2 Fraction module

If R is a PID and M is a finitely generated R-module, then $M \cong M_{\text{tors}} \oplus R^s$, where $s = \text{rank}(M)$. Let F be the field of fractions of R. Then FM is the F-module of fractions of M. That is, we define FM to be the equivalence classes of

$$\{(m, a) \in M \times R, a \neq 0\}$$

under the equivalence relation

$$(m, a) \sim (m', a') \qquad \text{iff } a'm = am'.$$

By defining addition and multiplication the same way we did for the field of fractions over R, we can make FM an abelian group.

There is a functor from R-modules to F-modules defined by mapping each element m of an R-module M to $\frac{m}{1}$, but we want the map from M to FM to be injective, and its kernel is actually M_{tors}. Since

$$FM \cong FM_{\text{tors}} \oplus FR^s \cong F^s,$$

the dimension of FM (over F) is $s = \text{rank}(M)$.

19.3 Modules over $\mathbb{F}[x]$

If $\mathbb{F}$ is a field, then $R = \mathbb{F}[x]$ is a Euclidean domain. Every nonzero ideal of R is generated by a unique monic polynomial. *Monic* means the coefficient in the highest-degree term is 1.

Since $\mathbb{F} \subset \mathbb{F}[x]$, every R-module M is also an $\mathbb{F}$-module, and therefore a vector space over $\mathbb{F}$.

For any nonconstant monic polynomial $g \in \mathbb{F}[x]$, we can use the notation $h \mapsto \overline{h} + gR$ for the canonical ring homomorphism from R to R/gR.

Lemma 19.3. *Any ring homomorphism from a field to a nonzero ring is injective.*

Proof. Let F be a field, S be a nonzero ring, and $f : F \to S$ be a ring homomorphism. Then $\text{Ker}(f) = 0$. □

Proposition 19.4. $\dim_{\mathbb{F}}(R/gR) = n = \deg(g)$. *Also, the elements*

$$\left\{1, \overline{x}, \overline{x}^2, \ldots, \overline{x}^{n-1}\right\}$$

form a basis for R/gR.

Proof. For any $h \in R$, $\overline{h}$ is a linear combination of those basis elements – to prove this, we use the fact that R is a Euclidean domain with the Euclidean function $\varphi(h) = \deg(h)$. We also need to prove that those basis elements are linearly independent, which is fairly easy. □

A finitely generated R-module M is torsion if and only if $\dim_{\mathbb{F}}(M)$ is finite.

Just like group actions are equivalent to group homo from a group to the symmetric group of the set they act on, R-modules are equivalent to ring homomorphisms from the underlying ring to the endomorphism ring of the module (or the aelian group).

20 3/4/2024 lecture

21 3/6/2024 lecture

Let $R = F[x]$, where F is a field. Then we can talk about R-module automorphisms in terms of finitely generated torsion R-modules M, linear operators $A : M \to M$, or $n \times n$ matrices over F. To understand this better, let's see how an automorphism of M can describe the linear operator on $V = F^n$ described by either a linear operator $A : V \to V$ or a matrix $[A]$.

Let $N \subset R^n$ be generated by the columns of $xI_n - A$, and let $Q = R^n/N$. Then there is a map $f : R^n \to R^n$ (called a presentation of Q) which is equivalent to left multiplication by $xI_n - A$ and whose image is N.

The first step for finding Q is to find the invariant factors of $xI_n - A$, which are nonconstant and monic. The determinant of $xI_n - A$ is the characteristic polynomial of A (which we'll denote P_A). To get that matrix into normal form, we left multiplied by elementary-row-operation matrices, whose determinants are 1, -1, or a unit. The determinant of the normal form matrix is $f_1 f_2 \cdots f_r$ (the product of all the invariant factors), so

$$P_A = u \cdot f_1 f_2 f_3 \cdots f_r$$

where u is a unit. But since we know P_A is monic, $u = 1$. HOW DOES THIS IMPLY THAT THE INVARIANT FACTORS OF Q ARE ALSO $f_1 \cdots f_r$???

Lemma 21.1. *Q and M are isomorphic as R-modules.*

Proof. Recall that

$$V \cong M \cong R/f_1R \oplus R/f_2R \oplus \cdots \oplus R/f_rR.$$

Let $\{v_1, v_2, \ldots, v_n\}$ be a basis for V, and let $[A]$ be $A : V \to V$ in that basis. Then we can construct an R-module homomorphism $g : R^n \to V$ which maps $(h_1, h_2, \ldots, h_n)$ to $h_1v_1 + h_2v_2 + \cdots + h_nv_n$. g must be surjective, and we can show by plugging in parameters that all columns of $xI_n - A$ are in the kernel of g ($N \subset \mathrm{Ker}(g)$). Knowing that allows us to define an R-module homomorphism $\overline{g} : Q \to M$ such that $g = \overline{g} \circ \pi$, where π is the canonical homomorphism from R^n to $R^n/N \cong Q$.

By decomposing Q into invariant factor form, we see that the dimension of Q is the sum of the degrees of the invariant factors $f_1, f_2, \ldots, f_r$. Then

$$\dim(Q) = \sum_i \dim(R/f_iR) = \sum_i \deg(f_i) = \deg(f_1 f_2 \cdots f_r) = \deg(P_A) = \dim(V) = n.$$

Since $\overline{g}$ is a surjective homomorphism which preserves dimension, it must be an isomorphism. □

Given a linear operator or a matrix, we want to know how to compute its invariant factors and its rational canonical form. Here's the general process for doing so:

1. Convert $xI_n - A$ to normal form, with monic polynomials on the diagonal.
2. Take the nonconstant polynomials on the diagonal, $f_1|f_2|\cdots|f_r$ ($r \leq n$) to be the invariant factors.

3. The RCF of that matrix/operator is the diagonal matrix whose diagonal is $C(f_1), C(f_2), \ldots, C(f_r)$.

For example, if

$$A = \begin{bmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix},$$

then the invariant factors of $xI_3 - A$ are $x - 2$ and $(x-2)^2$, so the RCF of $xI_3 - A$ is

$$\mathrm{RCF}(A) = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 0 & -4 \\ 0 & 1 & 4 \end{bmatrix}.$$

22 Topics to review

- Gauss' lemma
- UFDs
- Sylow's theorems (as practice – see 110AH notes)
- primitive, prime, and irreducible elements
- Adjoint functors
- Double check that definition of fraction modules is correct
- invariant factors and elementary divisors
- Rational Canonical Form (RCF) of a matrix