

Math 110BH Notes

Nathan Solomon

February 5, 2024

Contents

1	1/8/2024 lecture	2
1.1	Definition of a ring	2
1.2	Examples of rings	2
1.3	Properties of rings	3
1.4	The multiplicative group	3
2	1/10/2024 lecture	3
2.1	Integral domains & subrings	3
2.2	Ring homomorphisms	4
2.3	Ideals	4
3	1/12/2024 lecture	5
3.1	Quotient rings	5
3.2	Product of rings	5
4	1/17/2024 lecture	6
4.1	Chinese remainder theorem	6
4.2	Prime ideals	6
4.3	Maximal ideals	7
4.4	Posets and chains	7
5	1/19/2024 lecture	7
5.1	Field of fractions	7
5.2	Euclidean rings	8
6	1/22/2024 lecture	8
6.1	Factorization in integral domains	9
6.2	Irreducible elements	9
6.3	Prime elements	10
7	1/24/2024 lecture	10
7.1	Nifty trick	11
7.2	Unique factorization domains	11

8	1/26/2024 lecture	11
8.1	Noetherian rings	11
9	1/29/2024 lecture	12
10	1/31/2024 lecture	12
11	2/5/2024 lecture	12
11.1	Factorization of polynomials over fields	12

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 distributivity* – 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 $R = \text{End}(A) = \{f : A \rightarrow A \text{ is a homomorphism}\}$ 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 $S := \{f : X \rightarrow R\}$ 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 $R^\times = R \setminus \{0\}$. \mathbb{Q} and \mathbb{R} are examples of fields.

Here are some other 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 $\text{End}(A)^\times = \text{Aut}(A)$

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 $f : R \rightarrow S$ 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 $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ (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 right 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 $a_1, a_2, \dots, a_n \in R$, we call $Ra_1 + Ra_2 + \dots + Ra_n$ the *left ideal generated by* a_1, \dots, a_n . Replacing Ra_i by $a_i R$, we get the *right ideal generated by the* a_i s.

For any ring homomorphism $f : R \rightarrow S$, 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 $\pi : R \rightarrow R/I$ given by $\pi(a) = a + I$ is a surjective ring homomorphism, with $\text{Ker}(\pi) = I$.

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

Consider the function $f : \mathbb{R}[x] \rightarrow \mathbb{C}$ 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 $\text{Ker}(f)$ iff it is divisible by both $x - i$ and $x + i$. Therefore $\text{Ker}(f) = (x^2 + 1)\mathbb{R}[x]$, 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, $R := R_1 \times R_2 \times \dots \times R_n$, the 0 element in R is $(0_{R_1}, \dots, 0_{R_n})$, and similarly, $1_R = (1_{R_1}, \dots, 1_{R_n})$. If $e_1 \in R_1, e_2 \in R_2, \dots, e_n \in R_n$ are idempotents, the e_i s are orthogonal (meaning $e_i e_j = 0$ when $i \neq j$), the e_i s are all central ($e_i x = x e_i$ for any $x \in R$), and their sum is 1_R , then let the function $f : R \rightarrow$

$Re_1 \times Re_2 \times \cdots \times Re_n$ be defined by $f(a) = (ae_1, \dots, ae_n)$. 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, \dots, I_n are pairwise coprime ideals of a ring R , then for every tuple $(a_1, \dots, a_n) \in R^n$, 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 $j = 2$).

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, \dots, I_n are pairwise coprime ideals of a ring R , then the function

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

defined by

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

is surjective. If that function f is surjective, then $\text{Ker}(f) = I_1 \cap I_2 \cap \cdots \cap I_n$, 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 $\varphi : R \setminus \{0\} \rightarrow \mathbb{Z}^{\geq 0}$ 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:

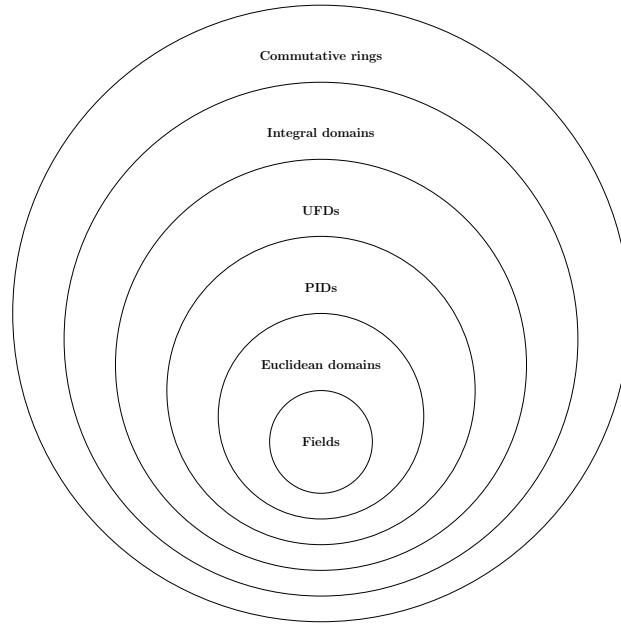
- \mathbb{Z} is a Euclidean domain because we can define a Euclidean function $\varphi(a) = |a|$.
- If \mathbb{F} is a field, then $R = \mathbb{F}[x]$ is a Euclidean domain because we can define $\varphi(f) = \deg(f)$.
- The *Gauss integers*, $R = \mathbb{Z}[i] \subset \mathbb{C}$, are a Euclidean domain 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 $\varphi : R \setminus \{0\} \rightarrow \mathbb{Z}^{\geq 0}$. Let $a \in I$ be a value of $I \setminus \{0\}$ 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 $r = aq \in I$, 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 $p \in R$ 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 $a = c_1 c_2 \cdots c_n$ (WHY DO WE ASSUME THIS IS FINITE???) for c_i irreducible in R . Conversely, if $aR = (c_1 R)(c_2 R) \cdots (c_n R)$, 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 $a = c_1 c_2 \cdots c_n = d_1 d_2 \cdots d_m$ (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 irreducible element, and suppose there exist $a, b \in R$ such that $c|ab$. Let $x_1 x_2 \cdots x_n = a$ and $y_1 y_2 \cdots y_m = b$ be unique factorizations of a and b . Since c divides ab , there is an element d such that $ab = cd$, and we can let $z_1 z_2 \cdots z_k$ 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 $a = c_1 c_2 \cdots c_n = d_1 d_2 \cdots d_m$ 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 $u \in R^\times$. 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 factorization 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, \dots, a_n such that $I = a_1R + a_2R + \dots + a_nR$)
- Every chain of ideals terminates, meaning if there is a sequence of ideals $I_1 \subset I_2 \subset I_3 \subset \dots$, 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 ($R[X_1, x_2, \dots, X_n]$) 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 $b, c \in R \setminus R^\times$ 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 Noetherian 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 $\{a_1, a_2, \dots, a_m\}$. 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.

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)
- $p \mid a_i$ 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 $f = g \cdot h$. 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 AND INCLUDE THE TWO EXAMPLES FROM CLASS