Ring Theory Lecture Notes

Nate Annau

Table of Contents

1. Rings

1.1. Rings

Lecture 1 Jan 6

1.1.1. Definition: Group

Recall that a group G is a set together with a binary operation $* : G \times G \to G$ such that

i) $*$ is associative
ii) $\exists 1 \in G$ such that $1 * a = a * a = a \forall a \in G$
iii) $\forall a \in G \exists a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = 1$.

1.1.2. Definition: Monoid

A **monoid** is similar to a group without requiring condition (iii).

1.1.3. Definition: Semigroup

A **semigroup** does not require conditions (ii) and (iii).

1.1.4. Example

i) $\mathbb{Z}_{>0}$ is the set of all nonnegative integers. This is a monoid.
ii) $\mathbb{Z}_{>0}$ is the set of positive integers. This is a semigroup.
iii) $(\mathbb{Z}, \times)$ is not a group, but it is a monoid.

1.1.5. Definition: Ring

A **ring** is a set R together with two binary operations, namely addition $(+)$ and multiplication $(\cdot)$ such that

i) $(R, +)$ is an abelian group.
ii) $(R, \cdot)$ is a monoid
iii) Addition and multiplication commute, i.e., $\forall a, b, c \in R$, we have

$$a \cdot (b + c) = a \cdot b + a \cdot c \qquad \text{and} \qquad (b + c) \cdot a = b \cdot a + c \cdot a.$$

If $a \cdot b = b \cdot a \forall a, b \in R$, then we say in addition that R is a **commutative ring**.

1.1.6. Definition: Additive and Multiplicative Identity

The identity element for addition is called the **additive identity** and is written as 0, and the identity element for multiplication is called the **multiplicative identity** and is written as 1.

1.1.7. *Proposition*

The multiplicative identity is unique.

Proof: Suppose 1 and $1'$ are distinct multiplicative identities. Then we know $11' = 1$ and $11' = 1'$, so $1 = 1'$.

□

1.1.8. Example

i) $R = \mathbb{Z}$
ii) $R = \mathbb{Q}, \mathbb{R}, \mathbb{C}$
iii) Let $n \in \mathbb{Z}^+$ and $R = M_n(\mathbb{R})$, the set of $n \times n$ real matrices. This is a ring with the usual addition and multiplication of matrices. This is an example of a noncommutative ring since $AB \neq BA$ in general.
iv) Let $n \in \mathbb{Z}^+ \setminus \{1\}$ and $R = \mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/n$. Recall multiplication here is defined by $(a \bmod n)(b \bmod n) := ab \bmod n$.

We now show this definition makes sense. Suppose $a \bmod n = a' \bmod n$ and $b \bmod n = b' \bmod n$. Then we can write $a = a' + kn$ and $b = b' + \ell n$. So $ab = (a' + kn)(b' + \ell n) = a'b' + mn$ for some $m \in \mathbb{Z}$.

The first condition is trivially satisfied from group theory. Further, it is easy to see that 1 is a multiplicative identity and multiplication is associative. Thus it only remains to show that multiplication distributes over addition, but this follows easily from the fact that this is the case in $\mathbb{Z}$. For the same reason, this is in fact a commutative ring.

1.2. Ring Properties

Lecture 2 Jan 8

1.2.1. *Proposition*

Let R be a ring. Then we have the following.
i) $a \cdot 0 = 0 \cdot a = 0 \forall a \in R$
ii) $(-a) \cdot b = a \cdot (-b) = -ab \forall a, b \in R$
iii) $(-a)(-b) = ab \forall a, b \in R$
iv) $a(b - c) = ab - ac, (b - c)a = ba - ca \forall a, b, c \in R$
v) $(-1)a = -a \forall a \in R$
vi) $(-1)(-1) = 1$.

Proof:

i) Notice $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$. Now since the group is closed under inverses, we have $a \cdot 0 = 0$. By a symmetric argument, $0 \cdot a = 0$.
ii) $(-a)b + ab = (-a + a)b = 0b = 0 \implies (-a)b = -ab$

iii) $(-a)(-b) - ab = (-a)(-b) + (-a)b = (-a)(-b+b) = (-a) \cdot 0 = 0$

iv) Exercise

v) Apply (2) with $b = 1$

vi) Apply (3) with $a = b = 1$

□

1.2.2. ***Corollary***

Suppose $0 = 1$. Then $R = \{0\}$ (this is called a **zero ring**.)

Proof: Let $a \in R$. Then $a = a \cdot 1 = a \cdot 0 = 0$.

□

1.2.3. ***Lemma***

Let R be a ring. Suppose $a \in R$ has a multiplicative inverse, meaning $\exists a' \in R$ such that $aa' = a'a = 1$. Then a' is the unique multiplicative inverse of a.

Proof: Suppose that b is another inverse of a. Then $a'ab = a'(ab) = a' \cdot 1 = a'$. Also, $a'ab = (a'a)b = 1 \cdot b = b$. Therefore $a' = b$.

□

1.2.4. ***Proposition***

Let $R^\times = \{a \in R : a \text{ has a multiplicative inverse}\}$. Then $R^\times$ is a group under multiplication.

Note this is called the **group of units**.

Proof: We only need to show that multiplication is defined on $R^\times$. Suppose $a, b \in R^\times$. Then $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a = a \cdot 1 \cdot a^{-1} = a \cdot a^{-1} = 1$. Similarly we can show $(ba)(a^{-1}b^{-1}) = 1$.

□

1.2.5. Example

If $R = M_n(\mathbb{R})$, then $R^x = \mathrm{GL}_n(\mathbb{R})$.

1.2.6. Example

Let $S \subset \mathbb{R}^n$. Let $C(S)$ be the set of all real valued continuous functions on S. Note any $f \in C(S)$ is a function $f : S \to \mathbb{R}$ is a function which is continuous at every point in S.

Define the operations

$$(f+g)(x) = f(x) + g(x)$$
$$(fg)(x) = f(x) \cdot g(x)$$

Then $C(S)$ forms a commutative ring, where the identities are the 0 function and the 1 function.

1.2.7. Example

More generally, let R be a ring and S any set. Define $F(S, R)$ as the set of all functions from S to R. Define

$$(f+g)(x) = f(x) + g(x)$$
$$(fg)(x) = f(x) \cdot g(x).$$

Note to prove this, it's better to use the sequential definition of continuity. Further, notice that $f(x) = x$ with $f : \mathbb{R} \to \mathbb{R}$ is an example of a function without an inverse.

1.2.8. Example

Let R be a ring. Let $M_n(R)$ be the set of all matrices of length n over R. If we take $A = (a_{ij})$ and $B = (b_{ij})$, we define $AB = (c_{ij})$ with $c_{ij} = \sum_n a_{in} b_{nj}$ Therefore it makes sense to talk about matrices over rings. In particular, we can talk about $M_n(\mathbb{Z}_m)$.

We can also construct a new ring by taking any set S and saying $R' = F(S, R)$.

1.2.9. Example: Difficulties of Ring Theory

Normal algebraic rules don't necessarily apply for rings. For instance, a nonzero number can have a square of 0 in a ring. If we take $R = \mathbb{Z}_4$ and $a = 2$, then $a^2 = 0$. Also, If we take $R = \mathbb{Z}_6$ and $a = 3$ so $a^2 = a$ but a is neither 0 nor 1.

1.3. Polynomial Rings

Lecture 3 Jan 10

1.3.1. Definition: Product of Rings

Let $0 \leq n \leq \infty$ be any integer. Let $\{R_i\}_{0 \leq i \leq n}$ be a collection of rings. We define

$$R = \prod_{i=0}^{n} R_i = \{\{a_i\} : a_i \in R_i\}$$

with ring operations

$$(a_i) + (b_i) = (a_i + b_i)$$
$$(a_i) \cdot (b_i) = (a_i \cdot b_i)$$

Then R becomes a ring.

Our multiplicative identity is $(1, 1, ..., 1)$ and our additive identity is $(0, 0, ..., 0)$.

1.3.2. Definition: Direct Sum of Rings

We can define

$$R' = \oplus_{i=0}^{n} R_i = \{(a_i) \in R : a_i = 0 \text{ for all but finitely many } i\}.$$

Note $R' \subseteq R$.

Notice that $R' = R$ if $n < \infty$, but $R' \neq R$ if $n = \infty$.

1.3.3. Exercise

Show that when $n = \infty$, R' is not a ring because it does not have a multiplicative identity.

Solution

Let $n = \infty$. Suppose by contradiction $1_{R'}$ is a multiplicative identity. Then $1_{R'}$ must eventually have a 0 entry by definition - call this entry i. Then consider $x \in R'$ where $x = (..., 1, ...)$ where the second 1 is in the ith position. But then $x1_{R'} = (..., 0, ...) \neq (..., 1, ...) = x$, so $1_{R'}$ cannot be an identity element.

1.3.4. Exercise

Let R be a ring. Consider

$$R' = \prod_{i=0}^{\infty} R_i \text{ where } R_i = R.$$

The operations are

$$(a_i) + (b_i) = (a_i + b_i)$$
$$(a_i)(b_i) := (c_i)$$

Define $c_i = \sum_{j+k=i} a_j \cdot b_k$.

To understand this, consider the j and k axes, so that the lines $j + k = i$ are the ones with slope -1.

Show this is a ring with additive identity $0 = (0, 0, ..., 0)$ and multiplicative identity $1 = (1, 0, ..., 0)$.

Solution

Consider $R' = \prod_{i=0}^{n} R_i$ for some $n \in \mathbb{N}$. Note that for $f = (a_0, ..., a_n), g = (b_0, ..., b_n) \in R'$ we have $f + g = (a_0 + b_0, ..., a_n + b_n) = (b_0 + a_0, ..., b_n + a_n) = g + f$, showing closure and commutativity of addition. Further notice $(a_0, ..., a_n) + (0, ..., 0) = (a_0, ..., a_n)$ so $(0, ..., 0)$ is indeed an identity. Then $(-a_0, ..., -a_n) + (a_0, ..., a_n) = (0, ..., 0)$ so additive inverses exist.

Now, $fg = \left(\sum_{j+k=0} a_j \cdot b_k, ..., \sum_{j+k=n} a_j \cdot b_k \right)$ so we have closure under multiplication, and note $f \cdot 1 = \left(\sum_{j+k=0} a_j \cdot b_k, ..., \sum_{j+k=n} a_j \cdot b_k \right) = (a_0, ..., a_n) = f$ so the multiplicative identity works.

1.3.5. Remark

If we return to the direct sum of rings with our new definition for multiplication, it becomes a ring.

Further, it is nothing but the ring of polynomials over R. I.e., if we fix an indeterminate x, we can define

$$a = a_0 + a_1 x + \cdots + a_n x^n.$$

We say that $\oplus R_i = R[x] =$ the polynomial being over R.

In fact, the definition of multiplication we defined is precisely the same as doing normal polynomial multiplication.

1.3.6. Definition: Degree of a Polynomial

The **degree of a polynomial** is the largest integer n such that $a_n \neq 0$.

1.3.7. Remark

We can then define a power series by considering $R = \prod R_i = R[[x]] = \{a_0 + a_1 x + \cdots\}$, with the same multiplication operation.

1.3.8. Definition: Polynomials and Power Series in n Variables

We can recursively define $R[x_1, ..., x_n] := R[x_1, ..., x_{n-1}]$ and $R[[x_1, ..., x_n]] := R[[x_1, ..., x_n]][[x_n]]$.

1.3.9. Example: Ring of Gaussian Integers

The **Ring of Gaussian Integers** is called $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\} \subset \mathbb{C}$. We can also consider $\mathbb{Q}[i] = \{a + ib : a, b \in \mathbb{Q}\} \subset \mathbb{C}$. Notice that this last ring has multiplicative inverses, and in fact has a square root of -1.

One advantage of ring theory is that we can study roots over rings rather than larger sets, to get other possible roots of numbers.

Gauss was investigating which integers can be written as a sum of two squares. He created this ring and said that an integer can be written as a sum of two squares if and only if it is the square of the norm of a Gaussian integer.

Gauss was also interested in figuring out how many integer lattice points are in a circle.

1.4. Subrings

Lecture 4 Jan 13

1.4.1. Definition: Subring

Let $(R, +, \cdot)$ be a ring and let $S \subseteq R$ be any subset. Then $(S, +, \cdot)$ is a called a subring if it is a ring under the binary operations of R.

1.4.2. *Proposition*

> Suppose $S \subseteq R$ is closed under subtraction and multiplication. Assume further that $1 \in S$. Then S is a subring of R.
>
> Importantly, this is not an only if.

Proof: In general, S is a subring if

i) $(S, +)$ is a subgroup of $(R, +)$
ii) $(S, \cdot)$ is a submonoid of $(R, \cdot)$
iii) Multiplication and addition commute in S

Then

i) Note closure under subtraction is enough to show that $(S, +)$ is a subgroup.
ii) Holds by our assumption that $1 \in S$ and S is closed under multiplication.
iii) Holds because it holds everything in R.

□

1.4.3. Example

i) $\mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C}$

ii) Let $R = \mathbb{Z}$ and consider $S =$ even integers $= \langle 2 \rangle$. Note $1 \notin S$, but since the previous proposition is not an if and only if, this alone is not enough to show it's not a ring. It is in fact not a subring, but this is a Homework question. Note $S \subset \mathbb{Z}$ is closed under subgroup multiplication.

iii) Consider $R = \mathbb{Z}/6$ and $S = \{0, 2, 4\} = \langle 2 \rangle$. S is closed under multiplication. Note that $4 \in S$ is the identity, since $0 \cdot 4 \equiv 0, 2 \cdot 4 \equiv 2, 4 \cdot 4 \equiv 4$ in the ring. This example shows that the unity of a subring may be different from that of the ring.

iv) Consider $R = \mathbb{Z}/6$ and $S = \{0, 3\}$. Note 3 is the unity of S and thus S is a subring.

1.4.4. Definition: Ring Center

Let R be a ring. Note that $Z(R)$, or the **center** of R, is defined to be

$$Z(R) = \{a \in R : ab = ba \forall b \in R\}.$$

1.4.5. *Proposition*

Let R be a ring. Then $Z(R)$ is a subring of R.

Proof: Apply the subring test. Suppose $a, b \in Z(R)$. Then $(a+b)c = ac + bc = ca + cb = c(a+b) \forall c \in R$. Thus we have closure under addition. Suppose $a \in Z(R)$. Then $(-a)b = -ab = -ba = b(-a) \forall b \in R$ so $-a \in Z(R)$. Thus we have closure under additive inverses. Clearly $1 \in Z(R)$. Finally, check $a, b \in Z(R) \implies ab \in Z(R)$, and then we get that R is a subring.

Moreover, $Z(R)$ is a commutative ring. Thus every ring contains a commutative subring.

□

1.4.6. Example: Center of Matrix Ring

Let R be a commutative ring. Let $S = M_n(R)$ with $n \geq 2$.

We claim that $Z(R) = R$, since the only matrices that commute with all others are diagonal matrices with constant entries, exactly what R is.

Let $k, i, j \leq n$. Consider the matrix $E_{ij}(1)$ where (i, j)th entry is 1 and all entries are zero. Suppose $A \in Z(S)$. Then $AE_{ij}(1) = E_{ij}(1)A \forall i, j$. Then $A \in R$.

In general, for any ring R, $Z(M_n(R)) = Z(R)$.

1.5. Integral Domains

1.5.1. Definition: Zero Divisor, Annihilator

Let $a \in R$. Then we say that a is a **zero divisor** if $\exists b \neq 0$ in R such that $ab = ba = 0$.

In this case, we say that b **annihilates** a, or that b is an **annihilator** of a.

1.5.2. Example: Zero Divisors

i) Let $R = \mathbb{Z}/6$, $a = 2$ and $b = 3$. Then $ab = 0$. Thus a and b are zero divisors.

ii) Let $R = \mathbb{Z}/4$ and $a = 2$. Then $a \cdot a = 0$ so a is a zero divisor. Suppose R is commutative. Then a and b are zero divisors. Then $ac = ca = 0$ for some $c \neq 0$. Thus $abc = acb = 0 = cab$.

iii) Let $R = \mathbb{Z}/6$. Then $a = 2, b = 3$, so a and b are zero divisors. Note $a + b = 5$. Is this a zero divisor? We claim that it cannot be because it is coprime to 6. In general if we let $a \in A^x$, then $ab = 0$ so $a^{-1}(ab) = 0 \Rightarrow a^{-1}(ab) = 0 \Rightarrow (a^{-1}a)b = 0 \Rightarrow b = 0$.

This shows that zero divisors are not closed under addition. Thus it has no obvious structure.

1.5.3. Definition: Unit

A **unit** of a ring is an invertible element for the multiplication of the ring. That is, $u \in R$ is a unit if $\exists v \in R$ such that $vu = uv = 1_R$.

Lecture 5 Jan 15

1.5.4. Definition: Integral Domain

A ring R is called an **integral domain** if it is commutative and has no nonzero zero divisors. In other words, the product of nonzero elements is nonzero.

1.5.5. Example: Integral Domain

The rings $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all integral domains.

1.5.6. *Proposition*

> Every subring of an integral domain is also an integral domain. Moreover, its unity element coincides with the unity element of the bigger ring.

Proof: Let $S \subseteq R$ be a subring. Let $a \in S$ be the identity element of S. Then for every $b \neq 0$ in S, we must have $ab = ba = b \Longrightarrow (a - 1)b = 0$.

Since $b \neq 0$ and R is an integral domain, we must have $a - 1 = 0$, or $a = 1$.

□

1.5.7. Example: Integral Domain — Arbitrary Real Functions

Let $R =$ All functions from $[0,1]$ to $\mathbb{R} = F([0,1], \mathbb{R})$. Let f be a nonzero and noninvertible element of in R. Define

$$g(x) = \begin{cases} 0 \text{ if } f(x) \neq 0 \\ 1 \text{ if } f(x) = 0 \end{cases}$$

Note $fg = 0$ with g nonzero, so this is not an integral domain.

1.5.8. Example: Integral Domain — Continuous Real Functions

Let $R = C([0,1])$ with

$$f(x) = \begin{cases} 0 \text{ if } 0 \leq x \leq \frac{1}{2} \\ x - \frac{1}{2} \text{ if } \frac{1}{2} \leq x \leq 1 \end{cases} \text{ and } g(x) = \begin{cases} \frac{1}{2} - x \text{ if } 0 \leq x \leq \frac{1}{2} \\ 0 \text{ if } \frac{1}{2} \leq x \leq 1 \end{cases}$$

Note $fg = 0$ but f and g are nonzero, so this is not an integral domain.

1.5.9. *Proposition*

> Let R be a commutative ring. then R is an integral domain if and only if for any $a, b, c \in R$ with $a \neq 0$, one has that $ab = ac \implies b = c$.

Proof: First suppose R is an integral domain, and suppose for $a, b, c \in R$ with $a \neq 0$ we have

$$ab = ac \iff a(b - c) = 0.$$

Then $b - c$ is a zero divisor, but since R is an integral domain, we must then have $b - c = 0$. But this implies $b = c$.

In the other direction, suppose that for any $a, b, c \in R$ with $a \neq 0$ we have $ab = ac \implies b = c$. Then if $c = 0$, we have $ab = 0 \Rightarrow b = 0$, implying that every zero divisor is zero. In other words, there are no nonzero divisors, showing R is an integral domain.

□

1.6. Division Rings

1.6.1. Definition: Division Ring

A ring R is called a division ring if $\forall a \neq 0, \exists b \in R$ such that $ab = ba = 1$.

1.6.2. Definition: Field

A ring R is called a **field** if it is a division ring and is commutative.

1.6.3. Remark

Observe we get more structure at each step:

Sets	Abelian Groups	Commutative Rings	Fields

One thing we might wonder is whether there are division rings that aren't fields. The following example illustrates this.

1.6.4. Example: Quaternion Space

Take $R = \mathbb{R}^4 = \mathbb{H}$. Then choose a basis $\{1, i, j, k\}$. Let $R = R \cdot 1 \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$. We define addition as follows: if $\alpha = a + bi + cj + dk$ and $\alpha = a' + b'i + c'j + d'k$, then $\alpha + \alpha' = (a + a') + (b + b')i + (c + c')j + (d + d')k$.

We define

$$ij = k = -ji$$
$$jk = i = -kj$$
$$ki = j = -ik$$

or in table form,

	1	i	j	k
1	1	i	j	k
i	i	-1	k	j
j	j	k	-1	$-i$
k	k	$-j$	i	-1

Notice that this ring is clearly not commutative.

Note if $a + bi + cj + dk \neq 0$, then

$$(a + bi + cj + dk)^{-1} = \frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2}$$

so this is a division ring.

1.6.5. Remark

Note that we can define a ring structure built from $\mathbb{R}^n$ where $n = 1, 2, 4, 8$, where $n = 2$ corresponds to $\mathbb{C}$, $n = 4$ corresponds to quaternions, and $n = 8$ corresponds to octonions. This is a very hard theorem to prove.

1.6.6. Exercise

$Z(\mathbb{H}) = \mathbb{R}$.

Solution

Suppose $q = a + bi + cj + dk \in Z(\mathbb{H})$. Then $qi = iq$ and $qj = jq$.

(Show $q = a$).

1.6.7. ***Proposition***

Let D be a division ring. Then $Z(D)$ is a field.

Proof: Note $Z(D)$ is a ring by Prop 1.4.5 and is commutative, so it is enough to show that $a \in Z(D)$ with $a \neq 0$ implies $a^{-1} \in Z(D)$. Let $b \in D$; we need to show $a^{-1}b = ba^{-1}$. But this is true iff $a(a^{-1}b) = a(ba^{-1})$. But this is the same as saying $b = aba^{-1} = baa^{-1} = b$.

□

Lecture 6 Jan 17

1.6.8. Example: Spheres

Note $S = \{(a_0, ..., a_n) : a_0^2 + \cdots + a_n^1\} \subset \mathbb{R}^{n+1}$. For example, S^1 is a circle (in addition, it's an abelian group).

1.6.9. Exercise

S^3 is a (nonabelian) group under multiplication of $\mathbb{H}$.

Solution

1.6.10. ***Theorem***

Let R be an integral domain. Then $R[x]$ is also an integral domain.

Proof: Let $f(x) \in R[x]$ and $f(x) = a_0 + a_1x + \cdots + a_nx^n$ where $a_i \in R$. If $a_n \neq 0$, then $\deg(f) = n$. In this case, a_n is the leading coefficient of f, i.e., $\ell(f)$. Note $f(x)$ is called a monic polynomial if $\ell(f) = 1$.

Suppose $g(x) \in R[x]$ such that $f(x)g(x) = 0$. Suppose by contradiction that $g(x) \neq 0$. We can write $g(x) = b_0 + b_1x + \cdots + b_mx^m$ with $b_m \neq 0$ (so $\deg g = m$). Note $(a_0 + a_1x + \cdots + a_nx^n)(b_0 + b_1x + \cdots + b_mx^n) = 0 \implies a_nb_m = 0$, a contradiction since R is an integral domain.

□

1.6.11. ***Corollary***

Suppose R is an integral domain. Then $R[x_1, ..., x_n]$ is always an integral domain $\forall n \geq 1$.

Proof: Use induction on n.

□

1.7. Finite Fields

1.7.1. ***Proposition***

$\mathbb{Z}/m$ is an integral domain for $m \geq 2 \iff m$ is a prime.

Proof: Suppose m is a prime. Suppose $(a \bmod m)(b \bmod m) = 0 \Rightarrow ab \bmod m \equiv 0 \Leftrightarrow m \mid ab \Leftrightarrow m \mid a$ or $m \mid b \Leftrightarrow a \bmod m \equiv 0$ or $b \bmod m \equiv 0$.

Conversely, suppose $\mathbb{Z}/m$ is an integral domain. It suffices to show that the only divisors of m are 1 and m. Suppose $\exists 1 < a < m$ such that $a \mid m \Rightarrow \exists 1 < b < m$ such that $ab = m$. But now $ab \bmod m \equiv 0 \equiv (a \bmod m)(b \bmod m) \Rightarrow a \bmod m \equiv 0$ or $b \bmod m \equiv 0 \equiv$ because $\mathbb{Z}/m$ is an integral domain. But now $m \mid a$ or $m \mid b$, a contradiction.

□

1.7.2. ***Proposition***

Let R be a finite ring. Then R is an integral domain $\iff R$ is a field.

Proof: We only need to show that $a \neq 0 \Rightarrow a$ has an inverse. Consider the set $S = \{a^m : m \geq 0\}$. Thus $|S| < \infty$ because $|R| < \infty$. Then $\exists 1 \leq m < n$ such that $a^m = a^n$. So $a^m(a^{n-m} - 1) = 0$. Since R is an integral domain and $a \neq 0$, we must have $a^{n-m} = 1 \Rightarrow aa^{n-m-1} = 1 \Rightarrow a^{n-m-1} = a^{-1}$.

□

1.7.3. ***Corollary***

$\mathbb{Z}_m$ is a field $\iff m$ is a prime.

Proof: Follows easily from above two propositions.

□

1.7.4. Remark

A natural question is to ask whether all finite fields are of the form $\mathbb{Z}_p$.

However, this is not the case, as the following example illustrates.

1.7.5. Example

Consider $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ and then the ring formed by $\mathbb{Z}_{m[i]}$ which is $\mathbb{Z}[i]$ reduced mod m in each coordinate.

For example, $\mathbb{Z}_3[i] = \{0, 1, 2, i, 1 + i, 2 + i, 2i, 1 + 2i, 2 + 2i\}$. Note this has cardinality 9 which is not prime.

1.7.6. Exercise

$\mathbb{Z}_3[i]$ is an integral domain.

Solution

1.7.7. Remark

There's something special about 3 here — a general prime p does not work.

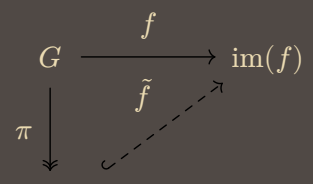
In fact, it must be a Gaussian prime, that is a prime congruent to 3 mod 4.

1.7.8. Example

Consider $\mathbb{Z}$. Note that intuitively, $\mathbb{Q}$ should be the smallest field containing $\mathbb{Z}$, since it's just the addition of inverses. We can generalize this in the following theorem.

1.7.9. *Theorem*

There exists a smallest field containing R. That is, $\exists$ a field F such that R is a subring of $F(R)$. Moreover, if R is a subring of a field K, then K contains $F(R)$ such that $R \hookrightarrow F(R)$ and $R \hookrightarrow K$ and $F(R) \hookrightarrow K$.



Proof: Let $S = \{(a, r) : a, r \in R, r \neq 0\} \hookrightarrow R \times R$.

Define the equivalence relation $(a, r) \sim (b, s)$ if and only if $as = br$ in R. Suppose $(a, r) \sim (b, s) \sim (c, t)$. Thus $as = br$ and $bt = cs$ and thus transitivity follows from

$$ats = ast = brt$$
$$crs = csr = btr = brt$$

We define $F(R) = S/\sim$. Define
- $(a, r) \cdot (b, s) = (ab, rs)$ and
- $(a, r) + (b, s) = (as + br, rs)$.

Then we claim
i) $F(R)$ is a ring with these operations
ii) R is a subring of $F(R)$

Note the additive identity is $(0, 1)$ and the multiplicative identity is $(1, 1)$. If $a \neq 0$, then $(a, a) \sim (1, 1)$. Consider this as an element of $F(R)$ by $(a, 1)$.

Note we think of the relation as $(a, r) \sim \frac{a}{r}$.

□

Lecture 7 Jan 22

1.7.10. Notation

$F(R)$ is called the field of fractions of R, or the quotient field of R.

1.7.11. Example

i) $F(\mathbb{Z}) = \mathbb{Q}$.
ii) Let D be an integer which is not a perfect square in $\mathbb{Q}$. Then $\mathbb{Z}\left(\sqrt{D}\right) = \left\{a + b\sqrt{D} \in \mathbb{C} : a, b \in \mathbb{Z}\right\}$. Then $\mathbb{Z}\left(\sqrt{D}\right)$ is a subring of $\mathbb{C}$.

1.7.12. Exercise

Take $R = \mathbb{Z}\left(\sqrt{D}\right)$.

Then $F(R) = \mathbb{Q}\left(\sqrt{D}\right) = \left\{a + b\sqrt{D} : a, b \in \mathbb{Q}\right\}$.

Solution

1.8. Characteristic

1.8.1. Definition: Characteristic

Let R be a ring. The **characteristic** of R is the smallest positive integer n such that $na = 0 \forall a \in R$. Note that this is repeated addition. If no such n exists, then we say that the characteristic of R is zero. We write this by $\text{char}(R) = n$.

1.8.2. *Proposition*

$\text{char}(R) = 0$ if and only if the order of 1 is ∞.

Proof: Suppose $\text{char}(R) = 0$. If the order of 1 is $n < \infty$, then $nx = (n \cdot x) = 0 \forall x \in R$, a contradiction. Conversely, suppose the order of 1 is ∞ and $\text{char}(R) = n > 0$. Then $n \cdot 1 = 0$, a contradiction.

□

1.8.3. *Proposition*

If $\text{char}(R) > 0$, then $\text{char}(R) =$ order of 1.

Proof: If $\text{char}(R) = n > 0$, then $n \cdot 1 = 0$. On the other hand, if $\exists 0 < m < n$ such that $m \cdot 1 = 0$, then $mx = (m \cdot 1)x = 0$, which implies $\text{ord}(1) = n$.

□

1.8.4. Example: Characteristic

i) $R = \mathbb{Z}$ then $\text{char}(R) = 0$.
ii) $R = \mathbb{Z}_6$ then $\text{char}(R) = 6$
iii) $R = \mathbb{Q}$
iv) $R = \mathbb{Z}/p$ where p is prime. Then $\text{char}\left(\mathbb{Z}_p\right) = p$.

1.8.5. ***Proposition***

Let R be an integral domain. Then either $\text{char}(R) = 0$ or $\text{char}(R)$ is prime.

Proof: If $\text{ord}(1) = \infty$, then we know char $R = 0$. Thus suppose $\text{ord}(1) = n > 0$. By contradiction, suppose n is not prime.

Thus we can write $n = m_1 m_2$ where $1 < m_1, m_2 < n$. Thus $n \cdot 1 = 0$. So $(m_1 \cdot 1)(m_2 \cdot 1) = n \cdot 1 = 0$. So either $m_1 \cdot 1 = 0$ or $m_2 \cdot 1 = 0$, contradiction.

□

1.8.6. ***Proposition***

Let R be an integral domain and let R' be a subring of R. Then $\text{char}(R') = \text{char}(R)$.

Proof: If $\text{char}(R) = 0$, then $\text{ord}(1) = \infty$ in R. But $1 \in R'$ is the identity element of R' then $\text{ord}(1) = \infty$ in R'. If $\text{ord}(1) = t > 0$ in R, then $\text{ord}(1) = t$ in R' as well.

□

1.8.7. Remark

The above proposition is false if R is not an integral domain. For example, take $R = \mathbb{Z}_6$ with $R' = \{0, 3\}$. Then $\text{char}(R) = 6$ and $\text{char}(R') = 2$.

1.8.8. Definition: F-vector space

Let F be a field. Let V be an abelian group. Then V is called an F-vector space if $\exists$ a map

$$\mu : F \times V \to V$$
$$\mu(a, v) \longmapsto av$$

such that

i) $a(v + w) = av + aw \forall a \in F, v, w \in V$
ii) $(a + b)v = av + bv \forall v \in V, a, b \in F$
iii) $a(bv) = (ab)v \forall a, b \in F, v \in V$
iv) $1 \cdot v = v \forall v \in V$

1.8.9. Notation

Whenever we write a finite field like $\mathbb{F}_p$ we mean $\mathbb{Z}_p$.

1.8.10. Example

Take $R = \mathbb{F}_p[x]$. Then R is an $\mathbb{F}_p$ vector space. Take $\alpha \in \mathbb{F}_p$ with $f(x) \in \mathbb{R}$ and $\alpha f(x)$ is usual multiplication in R.

A major problem is that $p \cdot n = 0$, which was never the case before, so we need to specially deal with this case.

Lecture 8 Jan 24

1.8.11. *Proposition*

For every ring R there exists a unique group homomorphism

$$\begin{aligned} \mathbb{Z} &\overset{\varphi_R}{\to} R \\ n &\longmapsto n \cdot 1 \end{aligned}$$

If R is an integral domain, then we can check
i) $\ker \varphi_R = \begin{cases} \langle p \rangle \\ 0 \end{cases}$

Thus every ring of characteristic zero contains $\mathbb{Z}$ canonically.

- g_f is an integral domain if $\operatorname{char} p$ contains $\mathbb{F}_p$ as a subring

1.8.12. Example

If $R = \mathbb{F}_p[x]$ and $F = F(R) = \left\{ \frac{f(x)}{g(x)} \mid g(x) \neq 0 \right\}$ we get an infinite ring of characteristic p.

2. Ideals

2.1. Ideals

2.1.1. Definition: Ideal

Let R be a ring. An **ideal** I in R is a subgroup of R under addition such that $\forall a \in I, b \in R$ we have $ab, ba \in I$.

Observe that we can visualize this as R with some abelian subgroup inside I, such that if we take any element outside of it and mulitply an element within I we are back in I.

2.1.2. Remark

Consider a field K and the vector spaces over itself; the only possibilities of subspaces are the trivial ones. However, if we consider a field, this is not true.

2.1.3. Definition

We say that I is a proper ideal if $I \neq \{1\}$.

2.1.4. Example

For $\mathbb{Z}$, the ideals are exactly all its subgroups. This is because each element of $\langle m \rangle$ times an integer must still be divisible by m.

2.1.5. Example

i) $R = \mathbb{Z}[x]$. Consider $S = 2\mathbb{Z} \hookrightarrow R$ Note this is only a subgroup of $\mathbb{Z}$. It's not a subring because it doesn't contain 1 (which it must because it's an integral domain).

ii) $R = \mathbb{Q}$, $S = \mathbb{Z}$, $\mathbb{Z} \hookrightarrow R$. S is a subring but not an ideal.

iii) $R = \mathbb{Z}$, $S = 2\mathbb{Z}$. S is not a subring but is an ideal.

2.1.6. Definition: Principal Ideal

Let R be a commutative ring and $a \in R$. Define $(a) = \{ba : b \in R\}$. Notice this is clearly closed under addition and if $ba \in R$ and $c \in R$, then $c(ba) = (cb)a \in (a)$ so it's closed under multiplication, showing (a) is an ideal.

In other words, it's an ideal generated by a single element.

Such an ideal is called a **principal ideal**.

2.1.7. Exercise

In general, let $a_1, ..., a_r \in R$. Define $(a_1, ..., a_r) = \{\alpha_1 a_1 + \cdots + \alpha_r a_r : \alpha_1, ..., \alpha_r \in R\}$. Then $(a_1, ..., a_r)$ is an ideal. (This is the same idea as the span of a subspace in a vector space)

Solution

If $\alpha_1 a_1 + \cdots + \alpha_r a_r \in (a_1, ..., a_r)$, then for $b \in R$ we have $b(\alpha_1 a_1 + \cdots + \alpha_r a_r) = \alpha_1(b_1 a_1) + \cdots + \alpha_r(b_r a_r) \in (a_1, ..., a_r)$, so this indeed an ideal.

2.1.8. Definition: Principal Ideal Ring

We say that a commutative ring R is a **principal ideal ring** (PIR) if every ideal of R is principal. We say that if R is a **principal ideal domain** (PID) if R is a PIR and an integral domain.

2.1.9. Example

i) $R = \mathbb{Z}$ is a PID

ii) $R = \mathbb{Z}_6$. Since every ideal of $\mathbb{Z}_6$ is a subgroup and hence cyclic, it follows that $\mathbb{Z}_6$ is a PIR, but not a PID.

In general, for any $\mathbb{Z}_n$, the ideals are exactly the subgroups.

Lecture 9 Jan 27

2.1.10. *Lemma*

Let R be an integral domain and $f(X), g(X) \in R[X]$. Then $\deg(f \cdot g) = \deg(f) \cdot \deg(g)$.

Proof: Let $m = \deg(f), n = \deg(g)$ such that

$$f(X) = a_0 + \cdots + a_m X^m, \quad g(X) = b_0 + \cdots + b_n X^n.$$

Therefore

$$f(X) \cdot g(X) = a_0 b_0 + \cdots + a_m b_n X^{m+n}$$

and note that $a_m b_n \neq 0$ since R is an integral domain, therefore $\deg(f \cdot g) = \deg(f) \cdot \deg(g)$.

□

2.1.11. ***Proposition***

$\mathbb{Z}[x]$ is not a principal ideal ring.

Proof: Let $I = (2, x)$; we claim that this is not principal.

Suppose by contradiction $I = (f(x))$. Then

$$f(x) = xh_1(x) + 2h_2(x) \tag{1}$$

(since it has to be in the ideal). But then

$$x = h_3(x)f(x) \tag{2}$$
$$2 = h_4(x)f(x) \tag{3}$$

by the defining property of an ideal.

We must have $f(x) \in \{\pm 1, \pm 2\}$ by our lemma. Suppose (ignoring the sign) that $f(x) = 2$. Then (2) gives a contradiction because the coefficients must then be even. On the other hand if $f(x) = 1$ we also have a contradiction because the right hand side has an even constant and the left hand side has an odd constant.

□

2.1.12. ***Theorem***

If R is a commutative ring such that $R[x]$ is a PID, then R is a field.

Proof: Since $R[x]$ is a PID, it is an integral domain, which shows R is an integral domain. Let $a \neq 0$ be a nonzero element of R. Look at $I = (a, x) \subset R[x]$. Since $R[x]$ is a PID, we can write $I = (f(x))$. Thus

$$f(x) = xh(x) + ag(x)$$
$$x = h_1(x)f(x)$$
$$a = h_2(x)f(x)$$

By the lemma, we must have $f(x) = \alpha \in R$ such that $\alpha\beta = a$ for some $\beta \in R$. By equation 2, $x = \alpha h_1(x) \Rightarrow 1 = \alpha\alpha'$ for some $\alpha' \in R$. Thus equation $1 \Longrightarrow \alpha = xh(x) + ag(x)$. Then if we set $x = 0$ we get $\alpha = ag(0) \in R$. Thus $1 = a(\alpha^{-1}g(0)) \Rightarrow a \in R^\times$.

□

2.1.13. Remark

The converse is also true, but the proof is more difficult.

2.1.14. Example: Ideals

i) If $R = \mathbb{Z}[x]$ and $I = (x)$ means I contains all polynomials with zero constant term.
ii) $I = \{\text{polynomials with constant even terms}\}$ is an ideal. This is generated by $I = (2, x)$
iii) $R = C([0,1])$. Take $I = \{\text{differentiable functions}\}$ - this is not an ideal.
iv) $R = C[\mathbb{R}]$.

$I = \{\text{all continuous functions on } \mathbb{R} \text{ whose graph passes through the origin}\}$ is an ideal.

2.1.15. Definition: Group Ring

We can create a new ring based on a group.

Let G be a monoid. Let K be a field. Then $K[G]$ is the k vector space with basis G. Then define

$$\left(\sum_{g\in G} a_g g\right) + \left(\sum_{g\in G} b_g g\right) = \sum_{g\in G}(a_g + b_g)g$$

$$\left(\sum_{g\in G} a_g g\right) \cdot \left(\sum_{h\in G} b_h h\right) = \sum\sum (a_g b_h)(g \cdot h)$$

where we note $a_g b_h$ is the field multiplication operation and $g \cdot h$ is the monoid operation.

2.1.16. Example

$k = \mathbb{Q}$, $G = \mathbb{Z}_{\geq 0}$, $\mathbb{Q}[\mathbb{Z}_{\geq 0}] = \mathbb{Q}[x]$.

Lecture 10 (Jesse transcribed) Jan 29

2.1.17. Definition: Nil-Radical of R

Let R be a ring and $a \in R$, then a is nilpotent if $a^n = 0$ for some $n > 0$. $\text{nil}(R)$ is the set of all nilpotent elements in R called the nil-radical of R.

2.1.18. ***Lemma:*** **Binomial Theorem**

Let R be a commutative ring and $a, b \in R$ then

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}.$$

Proof: By induction note that the $n = 1$ case is trivial. Then note that

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)(a+b)^n \\
&= (a+b)\sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i} \\
&= \sum_{i=0}^{n} \binom{n}{i} a^{i+1} b^{n-i} + \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i+1} \\
&= \sum_{j=1}^{n} \binom{n}{j-1} a^j b^{n-j+1} + \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i+1} \\
&= \sum_{i=0}^{n+1} \binom{n+1}{i} a^i b^{n+1-i}.
\end{aligned}$$

□

2.1.19. ***Proposition***

Assume R is a commutative ring, then $\operatorname{nil}(R)$ is an ideal.

Proof: Let $a, b \in \operatorname{nil}(R)$ such that $a^n = 0 = b^m$ for some $n, m > 0$. Then note that $(a+b)^{m+n} = 0$ by the binomial theorem, implying that $a + b \in \operatorname{nil}(R)$. If $a^m = 0$ and $b \in R$ then $(ab)^m = a^m b^m = 0$ such that $ab \in \operatorname{nil}(R)$. Therefore $\operatorname{nil}(R)$ is an ideal of R.

□

2.1.20. Example: $\operatorname{nil}(R)$ **is not an ideal generally**

Take $R = M_2(\mathbb{R})$ and $a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, b = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \in \operatorname{nil}(R)$. However note that $(a+b)^2 = I \notin \operatorname{nil}(R)$.

2.1.21. ***Theorem:*** **Fraction Ring**

Let R be a ring and I an ideal. Then R/I is a ring under the multiplication

$$(a \bmod I)(b \bmod I) = ab \bmod I.$$

Proof: Note it is sufficient to only show that the multiplication is well-defined since multiplication and addition are both induced from R. Now let $a \bmod I = a' \bmod I, b \bmod I = b' \bmod I$ such that $a = a' + \alpha, b = b' + \beta$ for some $\alpha, \beta \in I$. Then note that

$$\begin{aligned} ab \bmod I &= (a' + \alpha)(b' + \beta) \bmod I \\ &= (a'b' + \alpha b' + a'\beta + \alpha\beta) \bmod I \\ &= a'b' \bmod I \end{aligned}$$

since $\alpha b' + a'\beta + \alpha\beta \in I$ (because I is an ideal). Thus R/I is a ring.

□

2.1.22. Example: Fraction Ring

i) Let $R = \mathbb{Z}, I = m\mathbb{Z}$ then we have that $R/I = \mathbb{Z}_m$.
ii) Let $S = R[X], I = \langle I \rangle$ then we have $S/I = R$ since I is the set of all polynomials with zero constant terms.

2.1.23. ***Proposition***

Let R be a ring and I, J be two ideals, then:
i) $I + J := \{a + b | a \in I, b \in J\}$ is an ideal;
ii) $IJ := \{\alpha_1 a_1 + \cdots + \alpha_n a_n \mid \alpha_i \in I, a_i \in J\}$ is an ideal.

Proof: Let $\alpha \in R$ and $\beta \in I + J$ then $\beta = a + b$ for some $a \in I, b \in J$ such that $\alpha\beta = \alpha a + \alpha b \in I + J$ since $\alpha a \in I, \alpha b \in J$. Now let $\alpha \in R$ and $\beta \in IJ$ such that $\beta = \alpha_1 a_1 + \cdots \alpha_n a_n$ for $\alpha_i \in I, a_i \in J$. Then note that $\alpha\beta = \alpha\alpha_1 a_1 + \cdots \alpha\alpha_n a_n \in I$ since $\alpha\alpha_i \in I$. Therefore, $I + J$ and IJ are ideals of R.

□

2.1.24. Remark

If I, J are ideals of R, then $IJ \subseteq I, J \subseteq I + J$.

2.1.25. Definition: Ideal Generated by Set

Let $S = \{a_1, ..., a_n, ...\}$ be a possibly infinite set and let R be a commutative ring. Then

$$I = \{\alpha_1 a_1 + \cdots + \alpha_n a_n \mid \alpha_i \in R, a_i \in S\}$$

is an ideal generated by S. Note that S does not need to be finite, but the sum must be finite. We write $I = \langle a_1,...,a_n,... \rangle = \langle S \rangle$.

2.1.26. Example: Ideal Generated by Infinite Set

Let $R = \mathbb{Z}$ and $I = \langle \text{All Primes} \rangle$ then we have that $I = \mathbb{Z}$.

2.2. Ring Homomorphisms

2.2.1. Definition: Ring Homomorphism

Let $f : R \to S$ be a map between two rings. Then f is a ring homomorphism if

$$f(a+b) = f(a) + f(b), \quad f(ab) = f(a)f(b)$$

for any $a, b \in R$.

2.2.2. *Proposition*

Let $f : R \to S$ be a ring homomorphism then
i) $f(a^n) = f(a)^n$;
ii) $nf(a) = f(na)$;
iii) $f(0) = 0$;
iv) $\ker(f)$ is an ideal in R.

Proof: Note that (1), (2), and (3) are results of group theory. Now to show (4) let $a \in \ker(f), b \in R$ then $f(ab) = f(a)f(b) = 0$ since $f(a) = 0$. This implies $ab \in \ker(f)$, meaning that $\ker(f)$ is an ideal in R.

□

Lecture 11 Jan 31

2.2.3. *Proposition*

If $f : R \to S$ is a ring homomorphism, then $f(R)$ is a subring of S.

Proof:
- $f(a) \cdot f(b) = f(ab) \in f(R)$ if $f(a), f(b) \in f(R)$
- $f(1) \cdot f(a) = f(1 \cdot a) = f(a) \Rightarrow f(1)$ is the unity of $f(R)$

□

2.2.4. *Proposition*

Suppose that if $f : R \to S$ is a ring homomorphism such that f is an isomorphism (bijection) of sets. Then $f^{-1} : S \to R$ is also a ring homomorphism. In this case, we can say that f is an isomorphism of rings and we say that R and S are isomorphic as rings. We write this $R \approx S$.

Proof: We need to show that

i) $f^{-1}(a+b) = f^{-1}(a) + f^{-1}(b)$

ii) $f^{-1}(ab) = f^{-1}(a) \cdot f^{-1}(b)$

i) Notice

$$\begin{aligned} & f^{-1}(a+b) = f^{-1}(a) + f^{-1}(b) \\ \iff & f(f^{-1}(a+b)) = f(f^{-1}(a) + f^{-1}(b)) \\ \iff & a+b = f(f^{-1}(a)) + f(f^{-1}(b)) \\ \iff & a+b \end{aligned}$$

But $f(f^{-1}(a+b)) = a+b = f(f^{-1}(a) + f(f^{-1}(b)))$.

ii) Notice

$$\begin{aligned} & f^{-1}(ab) = f^{-1}(a) \cdot f^{-1}(b) \\ \iff & f(f^{-1}(ab)) = f(f^{-1}(a) \cdot f^{-1}(b)) \end{aligned}$$

□

2.2.5. Remark

A ring homomorphism may not take unity to unity. For example consider $S = \mathbb{Z}_6$ and $R = \{0, 3\} \hookrightarrow S$ where we are considering the inclusion map. But 3 is the unity element of R and not the unity element of S.

2.2.6. *Proposition*

Suppose $f : R \to S$ is a ring homomorphism which is nonzero. Assume that S is an integral domain. Then $f(1) = 1$.

Proof: We claim $f(1) \neq 0$. To see this, suppose $f(1) = 0$. Then $f(a) = f(1 \cdot a) = f(1) \cdot f(a) = 0 \forall a \in R$. So $f = 0$, a contradiction.

Now $f(1) = f(1 \cdot 1) = f(1)f(1) \Rightarrow f(1) - f(1)f(1) = f(1)(1 - f(1)) = 0$, so $1 - f(1) = 0 \iff f(1) = 1$ since S is an integral domain.

□

2.2.7. *Proposition*

Let $f : R \to S$ be a ring homomorphism and let $J \subset S$ be an ideal. Then $f^{-1}(J)$ is an ideal in R.

Proof: Let $a \in f^{-1}(J)$ and $b \in R$. Then $f(ab) = f(a) \cdot f(b) \in J$ since $f(a) \in J$ and $f(b) \in S$. Then $f(ba) = f(b)f(a) \in J$ as well. Thus $ab, ba \in f^{-1}(J)$.

□

2.2.8. Remark

The image of an ideal under a ring homomorphism may not be an ideal. We can for example take $R = \mathbb{Z}$ and $S = \mathbb{Q}$ and $f : \mathbb{Z} \hookrightarrow \mathbb{Q}$, the inclusion map. Take $I = m\mathbb{Z}$ where $m \neq 0$, which is an ideal in $\mathbb{Z}$ but not in $\mathbb{Q}$.

2.2.9. Example

Let $I \subset R$ be an ideal. Then the canonical map

$$\begin{aligned} \phi : R &\longrightarrow \frac{R}{I} \\ a &\longmapsto a \pmod I = a + I \end{aligned}$$

is a ring homomorphism.

To see this, note $\phi(ab) = ab \bmod I = (a \bmod I)(b \bmod I) = \phi(a)\phi(b)$.

2.2.10. *Proposition*

Let $I \subset R$ be an ideal and let $I \subset J$ be an inclusion of ideals (i.e., J is an ideal with I a subset of it). Then $\phi(J) \subset \frac{R}{I}$ is an ideal under the canonical map $\phi : R \to \frac{R}{I}$.

Proof: Take $a \in \phi(J)$ and $b \in \frac{R}{I}$. Then $\exists a' \in J$ and $b' \in J$ such that $\phi(a') = a$ and $\phi(b') = b$. But then $\phi(a'b') = \phi(a')\phi(b') = ab \in \phi(J)$.

□

2.2.11. *Theorem:* First Isomorphism Theorem for Rings

Let $f : R \to S$ be a ring homomorphism with kernel I. Then $\exists!$ injective ring homomorphism $\overline{f} : \frac{R}{I} \to S$ such that is commutative $\left(\overline{f} \circ \phi = f\right)$.

Proof: Factorization of f as $f = \overline{f} \circ \phi$ is shown in group theory, so we only need to show that $\overline{f}$ is a ring homomorphism. Thus

$$\overline{f}((a \bmod I)(b \bmod I)) = \overline{f}(ab \bmod I) := f(ab) = f(a)f(b) = \overline{f}(a \bmod I)\overline{f}(b \bmod I).$$

□

Lecture 12 Feb 3

2.2.12. *Lemma*

Let $f : A \to B$ be a ring homomorphism and let $I \subset A$ be an ideal such that $I \subset \ker(f)$. Then $\exists!$ ring homomorphism $\overline{f} : \frac{A}{I} \to B$ such that

Proof: By the previous theorem, f factors uniquely through $f' : \frac{A}{\ker(f)} \to B$, so this is a commutative diagram:

where $\overline{f} = f' \circ \alpha$.

□

2.2.13. Example: First Isomorphism Theorem for Rings

Consider the map

$$\begin{aligned} \phi : \mathbb{Z} &\longrightarrow \frac{\mathbb{Z}[i]}{i-2} \\ n &\longmapsto n \pmod{i-2} \end{aligned}$$

Define the inclusion maps $\iota : \mathbb{Z} \to \mathbb{Z}[i]$ and $\iota' : \mathbb{Z} \to \mathbb{Z}_5$. Then define $\overline{\phi} : \mathbb{Z}_5 \to \frac{\mathbb{Z}[i]}{(i-2)}$ by $\overline{\phi} \circ \iota' = \phi \circ \iota$.

Observe $\overline{\phi}(2) = i$ since $i - 2 = 0 \Rightarrow i^2 = 4 \Rightarrow 5 = 0$.

Note $\phi(5) = 5 = -(i-2)(2+i) \equiv 0$. (We can also argue $i - 2 = 0 \Longrightarrow i^2 = 4 \Rightarrow 5 = 0$).

Since $\overline{\phi}(2) = i$, we get that $\overline{\phi}(a + 2b) = a + bi \forall a, b \in \mathbb{Z} \Longrightarrow \overline{\varphi}(a + 2b) = a + bi \forall a, b \in \mathbb{Z}$. Thus $\overline{\varphi}$ is surjective.

Recall that the kernel of a ring homomorphism is an ideal. Now since $\mathbb{Z}_5$ is a field, its only possible ideals are 0 and $\mathbb{Z}_5$. Further, $\overline{\phi} \neq 0$, so the kernel must be $\mathbb{Z}_5$. Thus $\overline{\phi}$ is injective as well.

Thus $\frac{\mathbb{Z}[i]}{i-2} \cong \mathbb{Z}_5$.

2.2.14. Example

Let $R = \mathbb{Z}[i]$ and $I = \langle i-2 \rangle$ then let $\iota : \mathbb{Z} \to \mathbb{Z}[i]$ and $\iota' : \mathbb{Z} \to \mathbb{Z}_5$ be inclusions and let $\varphi : \mathbb{Z}[i] \to \frac{\mathbb{Z}[i]}{\langle i-2 \rangle}$ be the canonical map $a \mapsto a \bmod \langle i-2 \rangle$. Then define $\overline{\varphi} : \mathbb{Z}_5 \to \frac{\mathbb{Z}[i]}{\langle i-2 \rangle}$ such that $\overline{\varphi} \circ \iota' = \varphi \circ \iota$. Then note that $\overline{\varphi}(2) = i$ since $i - 2 = 0$ therefore $\overline{\varphi}(a + 2b) = a + bi$ such that $\overline{\varphi}$ is surjective. Then note that since $\overline{\varphi}(5) = 5 = (i-2)(i+2) = 0$ and $\mathbb{Z}_5$ is a field we must have that $\ker(\overline{\varphi}) \in \{\langle 0 \rangle, \mathbb{Z}_5\}$ and therefore $\ker(\overline{\varphi}) = \langle 0 \rangle$ and $\overline{\varphi}$ is injective. Therefore $\overline{\varphi}$ is a ring isomorphism as it is trivially a ring homomorphism.

2.2.15. Example

Take $R = \mathbb{Z}[x]$. Let I be all polynomials with even constant term. Note that $I = (x, 2)$.

Define $\phi : \mathbb{Z} \to \frac{\mathbb{Z}[x]}{(x,2)}$ by $\varphi(n) = n \pmod{x, 2}$. This gives a ring homomorphism (by the lemma). Note $\overline{\phi} : \mathbb{Z}_2 \longrightarrow \frac{\mathbb{Z}[x]}{(x,2)}$ is surjective because every polynomial $f(x)$ has the form $f(x) = xg(x) + C$ where C is a constant. Thus $f(x) = C \pmod{x}$ so $f(x) = C \pmod{I} = (x, 2)$.

So $\overline{\phi}$ is injective because $\mathbb{Z}_2$ is a field. So ϕ is an isomorphism.

2.3. Prime Ideals and Maximal Ideals

2.3.1. Definition: Prime Ideal

Let R be a commutative ring and $I \subset R$ a proper ideal. Then I is called a **prime ideal** if $\forall a, b \in R, ab \in I \Rightarrow a \text{ or } b \in I$.

2.3.2. Definition: Maximal Ideal

Let R be a commutative ring and $I \subseteq R$ be a proper ideal. Then I is called a **maximal ideal** if for every ideal $J \subset R$ such that $I \subseteq J$, we must have either $J = I$ or $J = R$.

2.3.3. ***Proposition***

Let R be a commutative ring and $I \subset R$ be an ideal. Then
i) I is prime $\Leftrightarrow \frac{R}{I}$ is an integral domain
ii) I is maximal $\Leftrightarrow \frac{R}{I}$ is a field

Proof:

i) Suppose I is a prime ideal. We need to show that $\frac{R}{I}$ is an integral domain. Let $\overline{a}, \overline{b} \in \frac{R}{I}$ such that $\overline{a}\overline{b} = 0 \Rightarrow ab \pmod I = 0 \Leftrightarrow ab \in I \Leftrightarrow a \in I$ or $b \in I \Leftrightarrow (a \pmod I) = 0$ or $(b \pmod I) = 0$.

Suppose $\frac{R}{I}$ is an integral domain. Let $a, b \in R$ such that $ab \in I$. Then $ab \pmod I = 0$ so $(a \bmod I)(b \bmod I) = 0 \overset{\text{int domain}}{\Leftrightarrow} a \pmod I = 0$ or $b \pmod I = 0 \Leftrightarrow a \in I$ or $b \in I$.

ii) Suppose I is a maximal ideal. We need to show $\frac{R}{I}$ is a field. Let $\overline{a} \in \frac{R}{I}$ be nonzero. Let $a \in R$ such that $a \bmod I = \overline{a}$. Thus $a \notin I$. Consider $J = I + (a)$. Since $a \notin I, I \subsetneq J$. But I is maximal so $J = R$, so $1 = \alpha + ba$ for some $\alpha \in I, b \in R$. But this means $1 = \alpha \pmod I + (b \bmod I)(a \bmod I)$, but this implies $\overline{a} \in \left(\frac{R}{I}\right)^\times$.

Suppose that $\frac{R}{I}$ is a field. Suppose $\exists$ an ideal $J \subset R$ such that $I \subsetneq J \subset R$, so $J \bmod I \neq 0$. But $\frac{R}{I}$ is a field, so $\frac{J}{I} = \frac{R}{I}$, but this implies $J = R$ (because we proved that the image of an ideal under a surjective map with certain conditions is also a ideal.)

□

2.3.4. Example

If $R = \mathbb{Z}$ and $I = m\mathbb{Z}$, then I is a prime ideal if and only if m is prime. We can see that in general, prime ideals are generalizations of prime numbers.

2.3.5. Definition: Prime Element

Let R be a commutative ring. The element $a \in R$ is called a **prime element** if (a) is a prime ideal.

2.3.6. ***Corollary***

I is a maximal ideal implies I is a prime ideal.

Proof: I maximal ideal $\Leftrightarrow \frac{R}{I}$ field $\Rightarrow \frac{R}{I}$ integral domain $\Leftrightarrow I$ prime ideal.

Note the converse is not true, for example take $R = \mathbb{Z}$ and $I = (0)$.

□

Lecture 13 Feb 5

2.3.7. *Proposition*

a is a prime element $\Leftrightarrow (a \mid bc \Rightarrow a \mid b \text{ or } a \mid c)$

Proof: a is a prime element if and only if

$$\begin{aligned} & a \mid bc \\ \Leftrightarrow\ & a\alpha = bc \text{ for some } \alpha \in R \\ \Leftrightarrow\ & bc \in (a) \\ \Leftrightarrow\ & b \in (a) \text{ or } c \in (a) \\ \Leftrightarrow\ & a\alpha = b \text{ or } a\beta = c \text{ for some } \alpha, \beta \in R \\ \Leftrightarrow\ & a \mid b \text{ or } a \mid c \end{aligned}$$

□

2.3.8. Remark

Why don't we have a notion of maximal numbers, like the way we have a notion of prime numbers? The reason is that in $\mathbb{Z}$, these notions are the same, which we will show later.

2.3.9. Example: Quotient Polynomial Ring

Consider $\mathbb{R}[x]$ with $I = (x^2 + 1)$.

Define ϕ by $\phi(a + bi) = a + bx$. Take for granted that ϕ is a ring homomorphism.

We claim that for all $f(x) \in \mathbb{R}[x], \exists a, b \in \mathbb{R}$ such that $f(x) = \phi(a + bi)$.

We proceed by induction on the degree of the polynomial. Let $f(x) \in \mathbb{R}[x]$. Our base case is if $\deg(f) \leq 1$, then $f(x) = a + bx \Rightarrow f(x) = \phi(a + bi)$ where $a, b \in \mathbb{R}$.

If $\deg f > 1$, write $f(x) = a_0 + a_1 x + x^2 g(x)$, where $g(x) \in \mathbb{R}[x]$. Then modulo I,

$$f(x) \bmod I = (a_0 + a_1 x) - g(x) \bmod I.$$

Since $\deg(g) < \deg(f), \exists \alpha \in \mathbb{C}$ such that $g(x) \bmod I = \phi(\alpha)$. So $f(x) \bmod I = \phi(a + bi) - \phi(\alpha) = \phi(a + bi - \alpha)$. Thus ϕ is surjective. Since $\mathbb{C}$ is a field, the kernel can only be $\{0\}$ or $\mathbb{C}$, and it's not trivial, so the kernel must be $\{0\}$. Thus ϕ is surjective and thus an isomorphism, which means $\frac{\mathbb{R}[x]}{I}$ is a field. But this occurs if and only if I is maximal by Proposition 2.3.3.

2.3.10. Exercise

Let R be any commutative ring and let $a \in R$. Define $\phi_a : R[x] \to R$ by $\phi_a(f(x)) = f(a)$. We define $f(a)$ for $a \in R$ by $f(a) = a_0 + a_1 a + \cdots + a_n a^n$. Check that ϕ_a is a ring homomorphism.

Solution

Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ and $g(x) = b_0 + b_1 x + \cdots + b_n x^n$, where some of the leading coefficients may be zero. Now $\phi_a(f+g) = \phi_a((a_0+b_0) + (a_1+b_1)x + \cdots + (a_n+b_n)x^n) =$ trivial.

2.3.11. Exercise

Let $\phi : R[x] \to R$ be defined by $\phi(x) = a$. Also $\overline{\phi} : \frac{R[x]}{x-a} \to R$ is defined by $\phi(\alpha) = \alpha \forall \alpha \in R \Rightarrow \overline{\phi}$ is surjective.

Suppose $\phi(f(x)) = 0 \Rightarrow f(a) = 0$. Show that $x - a$ divides $f(x)$.

Solution

2.3.12. Exercise

Show R is an integral domain $\Leftrightarrow (x-a)$ is a prime ideal in $R[x] \forall a \in R$.

Solution

Let R be an integral domain. Then let $f(x), g(x) \in R[x]$ such that $fg \in (x-a)$. So $fg = 0 \bmod I = (f \bmod I)(g \bmod I)$ and since R is an integral domain, $f = 0 \bmod I$ or $g = 0 \bmod I$.

In the other direction, let $(x-a)$ be a prime ideal in $R[x]$. Let $f, g \in R[x]$ with $fg \in (x-a)$. Then $fg \bmod I = 0 = (f \bmod I)(g \bmod I)$ and since $(x-a)$ is a prime ideal, at least of one of $f = 0 \bmod I$ or $g = 0 \bmod I$ is true.

2.3.13. Example

Let R be a commutative ring. Then $\exists!$ ring homomorphism $\phi : \mathbb{Z} \to R$ defined by $\phi(n) = n$.

If $\operatorname{char}(R) = 0$, then $\ker \phi = (0)$, so ϕ is a ring. But then $\mathbb{Z}$ is a subring of R. If $\operatorname{char}(R) = n > 0$, then $\ker \phi = n\mathbb{Z}$. So $\mathbb{Z}/n$ is a subring of R.

In particular, every integral domain canonically contains either $\mathbb{Z}$ or $\mathbb{Z}_p$ as a subring.

2.3.14. *Corollary*

Every integral domain if $\operatorname{char} p > 0$ is an $\mathbb{F}_p$ vector space.

2.3.15. ***Corollary***

Every field contains either $\mathbb{Q}$ or $\mathbb{F}_p$ as a subfield.

Proof: If a field contains $\mathbb{Z}$, it canonically contains $\mathbb{Q}$ as a subfield, because $\mathbb{Q}$ is a field of fractions of $\mathbb{Z}$.

□

3. Polynomial Reducibility

3.1. Reducibility

3.1.1. Remark

$\mathbb{Q}$ and $\mathbb{F}_p$ are called the prime fields. $\mathbb{Q}$ is of characteristic 0 and $\mathbb{F}_p$ is of characteristic p. Note $\mathbb{Q}$ is far easier to deal with.

3.1.2. Definition: Irreducible

An element a in a commutative ring R is called **irreducible** if $a \notin R^\times$ and $a = bc \Rightarrow b \in R^\times$ or $c \in R^\times$. In other words, it is not invertible and not the product of two noninvertible elements.

3.1.3. Example

If $R = \mathbb{Z}$, note the group of units is $R^\times = \{1, -1\}$.

Thus a is irreducible if and only if a is prime.

Lecture 14 Feb 10

3.1.4. *Proposition*

> Let R be an integral domain and let $a \in R$ be a prime element. Then a is irreducible.

Proof: Suppose $a = bc$, so either $a \mid b$ or $a \mid c$ by Prop 2.3.7. If $a \mid b$, then $b = a\alpha \Rightarrow b = bc\alpha \overset{\text{Prop 1.5.9}}{\Longrightarrow} 1 = c\alpha \Rightarrow a = a\alpha c \Rightarrow a(1 - \alpha c) = 0 \Rightarrow 1 - \alpha c = 0$ because R is an integral domain. Then $\alpha c = 1 \Rightarrow c \in R^\times$.

If $a \mid c$, then the same argument shows $b \in R^\times$.

□

3.1.5. Definition: Reducible

Let R be a commutative ring. Suppose $a \in R \setminus R^\times$ and a is not irreducible in R, that is, $a = bc \Rightarrow b \notin R^\times$ and $c \notin R^\times$. Then we say that a is reducible. Note this means that an element of a ring is either a unit, reducible, or irreducible.

3.1.6. Example: In general, irreducible $\not\Rightarrow$ prime

Let $R = \frac{\mathbb{C}[X,Y]}{(X^2-Y^3)}$. Let $a'(X,Y)$ be the image of a under the surjective map

$$\begin{aligned}\mathbb{C}[X,Y] &\longrightarrow R \\ x &\longmapsto x \bmod (X^2 - Y^3)\end{aligned}$$

We claim that a' is irreducible.

By contradiction, suppose a' were reducible. Then we could write $a'(X,Y) = f(X,Y)g(X,Y) \bmod (X^2 - Y^3)$ where $f(X,Y) \bmod I$ and $g(X,Y) \bmod I$ are not units. But this is the same as saying $a'(X,Y) = f(X,Y)g(X,Y) + h(X,Y)(X^2 - Y^3) \in \mathbb{C}[X,Y]$. But then $a'(X,Y) = f(X,0)g(X,0) + h(X,0)X^2 \in \mathbb{C}[X]$. But then since f and g are not units

Now we show that x is not prime in R.

$$\frac{R}{(x)} = \frac{\mathbb{C}[X,Y]}{(X^2 - Y^3, x)} = \frac{\mathbb{C}[Y]}{(Y^3)}.$$

In this ring, Y is a nonzero nilpotent element, so $\frac{R}{(x)}$ cannot be an integral domain. Thus X is not prime in R by Proposition 2.3.3.

3.1.7. *Proposition*

Let R be a PID. Then an ideal I is prime $\Leftrightarrow$ it is a maximal ideal.

Proof: Let I be a nonzero prime ideal. If $I = (a)$ then $a \neq 0$. Suppose $(a) \subsetneq (b) \Rightarrow a = bc$. But now since a is prime and $b \notin (a)$, we must have $c \in (a)$. Thus $c = a\alpha \Rightarrow a = bc = ba\alpha \Rightarrow a(1 - b\alpha) = 0 \Rightarrow b\alpha = 1 \Rightarrow b \in R^\times \Rightarrow (b) = R$.

□

3.1.8. *Proposition*

Let K be a field and $R = K[x]$. Notice there's a canonical map between $R \setminus \{0\}$ and $\mathbb{Z}_{\geq 0}$, which is just mapping a polynomial to its degree.

$f(x) \in R$ is irreducible $\Leftrightarrow$ it can't be written as a product of polynomials of lower (but positive) degrees.

Proof: If f is irreducible, then clearly we can't write it as a product of lower degree polynomials. Conversely, suppose f is not a product of polynomials of lower degree. Suppose $f = gh$. This implies $\deg(f) = \deg(g) + \deg(h)$. If $\deg(f) = \deg(g)$, then h must be a constant. If $\deg(f) = \deg(h)$, then g must be constant.

□

3.1.9. Example

Consider $\mathbb{Z}[x]$ and $f(x) = 2x^2 + 4 = 2(x^2 + 2)$. Then f is reducible.

Now consider $\mathbb{Q}[x]$ and still consider $f(x) = 2(x^2 + 2)$. This time f is irreducible by the previous proposition, since we can't break the quadratic term into two linear terms.

3.1.10. *Proposition*

Let $R = K[x]$ where K is a field. If $f(x)$ has a zero in K, then either $f(x)$ is linear or $f(x)$ is reducible.

Proof: Look at the ring homomorphism $\phi : R[x] \to K$ given by $\phi(f(x)) = f(a)$. We saw that this defines a ring isomorphism $\overline{\phi} : \frac{K[x]}{x-a} \xrightarrow[\sim]{} K$ where $a \in K$ such that $f(a) = 0 \Rightarrow f(x) \equiv 0 \bmod (x - a) \Rightarrow (x - a) \mid f(x) \Rightarrow f(x)$ is reducible.

□

Lecture 15 Feb 12

3.1.11. *Proposition*

Suppose $\deg(f) \in \{2, 3\}$. Then f is reducible if and only if f has a zero.

Proof: Suppose f is reducible. This implies $f = gh$, but now at least one of g and h are linear. But every linear polynomial has a zero in the field $\Rightarrow$ f has a zero.

□

3.1.12. Example

i) Take $R = \mathbb{Z}_3[x]$ and take $f(x) = 1 + x^2$. Notice $f(0) = 1, f(1) = 2, f(2) = 2$, so f never vanishes. Thus f is irreducible.

   This is actually the same result as this exercise, just from a different persepective.

ii) Take $R = \mathbb{Z}_5[x]$. Let $f(x) = 1 + x^2$. Notice $f(0) = 1, f(1) = 2, f(2) = 5 = 0$ so $f(x)$ is reducible. We can reinterpret this as well: notice $\frac{\mathbb{Z}_5[x]}{1+x^2} = \mathbb{Z}_5[i]$.

iii) Take $R = \mathbb{Q}[x]$ and $f(x) = x^4 + 2x^2 + 1$. We can observe $f(x) = (x^2 + 1)^2$ so it is reducible, despite f not having any zeros in $\mathbb{Q}$. This shows the limitations of the previous proposition.

3.2. Polynomial Zeros

3.2.1. *Theorem*

Let $R = K[x]$ where K is a field. Let $f(x), g(x) \in R[X]$ such that $g(x) \neq 0$. Then $\exists!$ polynomials $q(x), r(x)$ such that $f(x) = q(x)g(x) + r(x)$ where $r(x) = 0$ or $\deg(r) < \deg(g)$.

Proof: Proceed by induction on $\deg(f)$.

i) If $\deg(f) < \deg(g)$, then take $q = 0$ and $r = f$.

ii) If $\deg(f) \geq \deg(g)$, write $f(x) = a_0 + a_1x + \cdots + a_nx^n$ and write $g(x) = b_0 + b_1x + \cdots + b_mx^m$. Define $f_1(x) = f(x) - b_m^{-1}a_nx^{n-m}g(x)$. Then $\deg(f_1) < n$ so $\exists$ polynomials $q_1(x)$ and $r_1(x)$ such that $f_1(x) = q_1(x)g(x) + r_1(x)$. Thus

$$f(x) = b_m^{-1}a_nx^{n-m}g(x) + q_1(x)g(x) + r_1(x) = (b_m^{-1}a_nx^{n-m} + q_1(x))g(x) + r_1(x).$$

Then we can take $q(x) = b_m^{-1}a_mx^{n-m} + q_1(x)$ and $r(x) = r_1(x)$.

To show uniqueness, suppose $f(x) = q(x)g(x) + r(x) = q'(x)g(x) + r'(x) \Rightarrow (q(x) - q'(x))g(x) = r(x) - r'(x)$. By comparing the degrees on both sides, we must have $q(x) - q'(x) = 0$ and $r(x) = r'(x) = 0$.

□

3.2.2. Example

Let $R = \mathbb{Z}_5[x]$ and $f(x) = 3x^4 + x^3 + 2x^2 + 1$ and $g(x) = x^2 + 4x + 1$. We can divide $f(x)$ by $g(x)$ using polynomial division while accounting for being in $\mathbb{Z}_5$, and we should get $3x^2 + 4x + 3$ with remainder $4x - 2$. Thus overall $3x^4 + x^3 + 2x^2 + 1 = (3x^2 + 4x + 3)(x^2 + 4x + 1) + (4x + 3)$.

3.2.3. *Corollary*

Suppose $f(x) \in K[x]$ and $a \in K$. Then $f(a) = 0 \iff (x - a) \mid f(x)$.

Proof: Note the $\Longleftarrow$ direction is trivial. In the reverse direction, $f(x) = q(x)(x - a) + \xi(x) \Rightarrow \xi(x) = \alpha \in R$. So $f(x) = q(x)(x - a) + \alpha \Rightarrow 0 = f(a) = \alpha \Rightarrow f(x) = q(x)(x - a) \Rightarrow (x - a) \mid f(x)$.

□

3.2.4. *Corollary*

If $f(x) \in K[x]$ and $a \in K$ then $f(a)$ is the remainder for division of $f(x)$ by $(x - a)$.

Proof: Since $f(x) = q(x)(x - a) + r(x)$ we have $f(a) = r(x) \in R$.

□

3.2.5. Definition: Multiplicity

Let $f(x) \in K[x]$ with $a \in K$. Suppose $f(a) = 0$. Then the **multiplicity** of a as a zero of $f(x)$ is the largest integer such that $(x-a)^n \mid f(x)$.

3.2.6. *Proposition*

Let K be a field. If $\deg(f) = n \wedge f \neq 0$ in $K[x]$, then f has at most n zeros counting multiplicity.

Proof: Suppose $f(a) = 0$. Then $f = g(x)(x-a)$ by Corollary 2.5.3. By induction, g has at most $n-1$ zeros. And zeros of $f \subseteq \{\text{zeros of } f\} \cup \{a\}$.

□

Lecture 16 Feb 14

3.2.7. Example

If $K = \mathbb{C}$ and $f(x) = x^n - 1$ then write $\omega = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n}) \in \mathbb{C}$. So $\omega^n = \cos((2\pi \cdot n)n) + i\sin(\frac{2\pi \cdot n}{n}) = 1 \implies (\omega^i)^n = (\omega^n)^i = 1 \implies f(\omega^i) = 0$ for $0 \leq i \leq n-1$. By the theorem, roots of f are $\{\omega^i : 0 \leq i \leq n-1\} \cong \mathbb{Z}_n$. THese are called the nth roots of unity, and ω is called a primitive root of unity.

3.3. Primitives

3.3.1. Remark

We now spend some time considering the following commutative diagram:

3.3.2. Definition: Primitive

Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$. Let

$$\text{cont}(f) = \text{content of } \ f = \gcd(|a_0|, ..., |a_n|) \in \mathbb{Z}_{\geq 1}$$

We say that f is **primitive** if $\text{cont}(f) = 1$. In general, $f = \text{cont}(f) f'$ where f' is primitive.

3.3.3. *Lemma:* Gauss's Lemma

The product of primitive polynomials is primitive.

Proof: Let $h = fg$ where f and g are primitive. Suppose h is not primitive. Then $\exists p$ a prime such that $p \mid h$.

We will write $\overline{f} = f \bmod p$. Then $\overline{h} = 0 \implies \overline{f}\,\overline{g} = 0 \implies \overline{f} = 0$ or $\overline{g} = 0$ so either $p \mid \text{cont}(f)$ or $p \mid \text{cont}(g)$. $\implies\Longleftarrow$

□

3.3.4. *Proposition*

Let $f(x) \in \mathbb{Z}[x]$ be a nonconstant polynomial. Suppose f is primitive. Suppose f is reducible over $\mathbb{Q}$. Then f is reducible over $\mathbb{Z}$.

Proof: Suppose $f(x) = g(x)h(x)$ where $g(x), h(x) \in \mathbb{Q}[x]$. By clearing the denominators of the coefficients of g and h, we get that $ag(x), bh(x) \in \mathbb{Z}[x]$ for some $a, b \in \mathbb{Z}_{>0}$. Then we get $abf(x) = ag(x)bh(x) = c_1 g'(x) c_2 h'(x)$ where g', h' are primitive. Thus $abf(x) = (c_1 c_2) g'(x) h'(x)$.

We claim that $\text{cont}(abf) = ab$ (shown by below exercise). Thus $\text{cont}(abf) = \text{cont}(c_1 c_2 g'(x) h'(x)) \implies ab = c_1 c_2$. Thus $f(x) = g'(x)h'(x) \implies f$ is reducible over $\mathbb{Z}$.

□

3.3.5. Exercise

Let $a_0, \ldots, a_n \in \mathbb{Z}$ where $\gcd(a_0, \ldots, a_n) = 1$. Then if $b \in \mathbb{Z}$ we have $\gcd(ba_0, \ldots, ba_n) = b$.

Solution

3.3.6. Example

Take $f(x) = 6x^2 + x - 2$. Note by the Quadratic Formula, the roots are given by

$$\begin{aligned} \alpha &= \frac{-1 \pm \sqrt{1 + 2 \cdot 4 \cdot 6}}{12} \\ &= \frac{-1 \pm 7}{12} = \frac{1}{2}, -\frac{2}{3}. \end{aligned}$$

Thus $f(x) = 6\left(x - \frac{1}{2}\right)\left(x + \frac{2}{3}\right)$, so $f(x)$ is reducible over $\mathbb{Z}$ by the previous proposition.

3.3.7. Example

Consider $f(x) = 2x^2 + 2 = 2(x^2 + 1)$. This is reducible over $\mathbb{Z}$ and irreducible over $\mathbb{Q}$ (since 2 is a unit in $\mathbb{Q}$ but not in $\mathbb{Z}$).

3.3.8. *Proposition*

Suppose that $f(x) \in \mathbb{Z}[x]$ is a monic polynomial. If f is irreducible over $\mathbb{Q}$, then it is irreducible over $\mathbb{Z}$.

Proof: Suppose $f(x) = g(x)h(x)$. Then this gives a factorization of f over $\mathbb{Q}$ as well.

□

3.3.9. ***Theorem***

If K is a field, then $K[x]$ is a PID. (Converse of Theorem 2.1.12.)

Proof: Let $I \subseteq K[x]$ be an ideal. If $I = (0)$, we have nothing to prove. Thus we can assume $I \neq 0$. Let $g(x) \in I$ be a polynomial of smallest degree in I. Now take any $f(x) \in I$. We have $f(x) = q(x)g(x) + r(x)$ where $r(x) = 0$ and $\deg(r) < \deg(g)$. If $r(x) \neq 0$, then we get a contradiction because $r(x) \in I$ and $\deg(r) < \deg(g)$.

□

3.4. Reducibility with $\mathbb{Z}_p$

Lecture 17 (Jesse transcribed) Feb 19

3.4.1. ***Theorem***

Suppose $f(X) \in \mathbb{Z}[X]$ is a polynomial of positive degree and p is prime such that $\deg(f) = \deg\left(\overline{f}\right)$. Then if $\overline{f}$ is irreducible over $\mathbb{Z}_p$ we have that f is irreducible over $\mathbb{Z}$.

Proof: $f(X) = af'(X)$ where f' is primitive. Seeking a contradiction let $f(X)$ be reducible over $\mathbb{Q}$. We have that $\overline{f}$ is irreducible over $\mathbb{Z}_p$ if and only if $\overline{f'}$ is irreducible over $\mathbb{Z}_p$ since $a \in \mathbb{Z}_p^\times$. So without loss of generality let f be primitive. Since f is reducible over $\mathbb{Q}$ we must have f is reducible over $\mathbb{Z}$. So $f = gh$ where $\deg(g), \deg(h) < \deg(f)$. $\overline{f} = \deg(g)\deg(h)$ so $\overline{f}$ is reducible over $\mathbb{Z}_p$ which is a contradiction. Therefore f must be irreducible over $\mathbb{Z}$.

□

3.4.2. Example: Reducible over $\mathbb{Z}$ and irreducible over $\mathbb{Z}_2$

Let $f(X) = (2X + 1)(X + 1) \in \mathbb{Z}[X]$. f is clearly reducible in $\mathbb{Z}$ but $\overline{f} = X + 1 \in \mathbb{Z}_2[X]$.

3.4.3. ***Proposition***

$f(X) = X^4 + 1$ is reducible over $\mathbb{Z}_p$ for any p.

Proof: First let $p = 2$ then $(X^4 + 1) = (X^2 + 1)^2 \in \mathbb{Z}_2[X]$. Now let $p \neq 2$ and consider the following:

(**Case 1**) Assume there exists some $a \in \mathbb{Z}_p$ such that $a^2 = 2$ then

$$\begin{aligned}(X^2 + aX + 1)(X^2 - aX + 1) &= (X^2 + 1)^2 - (aX)^2 \\ &= X^4 + 2X + 1 - (aX)^2 \\ &= X^4 + 1.\end{aligned}$$

(**Case 2**) Now let there exists some $a \in \mathbb{Z}_p$ such that $a^2 = -2$ then

$$\begin{aligned}(X^2 + aX - 1)(X^2 - aX - 1) &= (X^2 - 1)^2 - (aX)^2 \\ &= X^4 - 2X + 1 - (aX)^2 \\ &= X^4 + 1.\end{aligned}$$

(**Case 3**) Finally assume there exists $a \in \mathbb{Z}_p$ such that $a^2 = -1$ then

$$(X^2 + a)(X^2 - a) = X^4 - a^2 = X^4 + 1.$$

Thus it is sufficient to show that for any $p \neq 2$ there exists some $a \in \mathbb{Z}_p$ such that $a^2 \in \{-1, \pm 2\}$.

3.4.4. ***Lemma***

Let p be any prime then there exists some $a \in \mathbb{Z}_p$ such that $a^2 \in \{-1, \pm 2\}$.

Proof: If $p = 2$ then $1 = -1$ so $1^2 = (-1)^2 = \pm 1$. Now let $p \neq 2$ and consider the map $\theta : \mathbb{Z}_p^\times \to \mathbb{Z}_p^\times$ where $\theta(a) = a^2$ defines a group homomorphism. Note that

$$\ker(\theta) = \{a \in \mathbb{Z}_p \mid a = \pm 1\}$$

such that $|\ker(\theta)| = 2$. Let $H = \mathrm{Im}(\theta)$ then $\left[\mathbb{Z}_p^\times : H\right] = 2$. Suppose $-1, 2 \notin H$ then we have that $(-1)H = 2H$ so $(-1)2H = (-2)H = H$. Thus we have that $-2 \in H$.

□

Thus it follows that $f(X)$ is reducible over $\mathbb{Z}_p$.

□

3.4.5. Definition: Eisenstein Polynomial

Let $f(X) = a_0 + \cdots + a_n X^n \in \mathbb{Z}[X]$. $f(X)$ is an Eisenstein polynomial if there exists some prime p such that $p \nmid a_n$, $p \mid a_i$ for $i < n$, and $p^2 \nmid a_0$. If the conditions are satisfied we say that f is p-Eisenstein.

3.4.6. Example: Eisenstein Polynomial

Let $f(X) = X^3 + 5X^2 + 15X + 5$ is 5-Eisenstein.

3.4.7. *Proposition*

$f(X) = X^4 + 1$ is irreducible over $\mathbb{Z}$.

Proof: $f(X) = X^4 + 1$ is irreducible if $f(X + 1)$ is irreducible. We have

$$f(X + 1) = X^4 + 4X^3 + 6X^2 + 4X + 2$$

which is p-Eisenstein and therefore is irreducible in $\mathbb{Q}$ by previous theorem. Since f is a monic polynomial this implies f is irreducible over $\mathbb{Z}$.

□

3.4.8. Example: Irreducible in $\mathbb{Z}_p$ implies irreducible in $\mathbb{Z}$

Let $f(X) = 21X^3 - 3X^2 + 2X + 8 \in \mathbb{Z}[X]$. Then note that $\deg(f \bmod 2), \deg(f \bmod 3) \neq \deg(f)$. However consider $\overline{f} = f \bmod 5$ since

$$\overline{f}(X) = X^3 + 2X^2 + 2X + 3$$

such that $\deg\left(\overline{f}\right) = \deg(f)$. Then note $\overline{f}(X) \neq 0$ for any $X \in \mathbb{Z}_5$ such that $\overline{f}$ is irreducible in $\mathbb{Z}_5$ implying that f is irreducible over $\mathbb{Z}$.

Lecture 18 Feb 21

3.4.9. ***Theorem***

Eisenstein polynomials are irreducible over $\mathbb{Q}$.

Proof: Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$. Suppose that f is reducible over $\mathbb{Q}$ by Proposition 2.6.8. Then f is reducible over $\mathbb{Z}$, and we can write $f = cf'$ where $c = \text{cont}(f)$ and f' is primitive. Thus f' is reducible over $\mathbb{Z}$ by Proposition 2.6.4.

Now we can write $f(x) = g(x)h(x)$ where $1 \leq \deg(g), \deg(h) < n$. Let $f(x) = a_0 + a_1x + \cdots = a_nx^n$ and write $g(x) = b_0 + b_1x + \cdots + b_rx^r$ and $h(x) = c_0 + c_1x + \cdots + c_sx^s$. Thus we have $a_0 = b_0c_0$ and $a_n = b_rc_s$.

3.4.10. ***Lemma***

Let $f(x) = \sum_{i=0}^{n} a_ix^i$ be an Eisenstein polynomial. Let $c = \text{cont}(f)$. Write $f(x) = cg(x)$, where $g(x)$ is a primitive polynomial. Then $g(x)$ is also Eisenstein.

Proof: Write $g(x) = b_0 + b_1x + \cdots + b_nx^n$. Then $a_i = cb_i \forall i$. Notice $p \nmid\Rightarrow p \nmid b_n$ and $p \nmid c$. If $p \mid a_i = cb_i \Rightarrow p \mid b_i \forall c < n$. Finally, if $p^2 \mid bc \Rightarrow p^2 \mid a_0 = cb_0 \Longrightarrow\Longleftarrow$.

□

i) Since $p \mid a_0$ but $p^2 \nmid a_0$, it must divide either b_0 or c_0 but not both.
ii) We also have $p \nmid a_n = b_rc_s$, so $p \nmid b_r$ and $p \nmid c_s$. Thus there exists a positive integer t such that $p \mid b_t$.
iii) Look at

$$a_l = b_tc_0 + (b_{t-1}c_1 + \cdots + b_1c_{t-1} + b_0c_t) = b_tc_0 + \alpha.$$

Then $p \mid \alpha$ since $p \mid b_i \forall i < t$, but $p \mid a_t$ since $t \leq r < n$ so $p \mid b_tc_0$, but $p \nmid b_t$ and $p \nmid c_0$. Contradiction.

□

3.4.11. Example

Consider the Eisenstein polynomial $x^4 + 4x^3 + 6x^2 + 4x + 2/$ This is irreducible over $\mathbb{Z}$ because it's Eisenstein, so it's reducible mod p for all p.

Note the above theorem is to have an additional criterion for irreducibility in addition to Theorem 2.6.10, for example.

We might think that this is a very special case unlikely to come up, but we can easily construct Eisenstein polynomials, which shows important examples. For example, consider the following corollary.

3.4.12. ***Corollary***

There exists an irreducible polynomial over $\mathbb{Z}$ of every degree: $f(x) = x^n + p$.

3.4.13. ***Proposition***

Let p be a prime. Consider $\phi_p(x) = 1 + x + \cdots + x^{p-1} \in \mathbb{Z}[x]$. We claim $\phi_p(x)$ is irreducible over $\mathbb{Z}$.

Proof: Notice $\phi_p(x) = \frac{x^p-1}{x-1}$. Note this isn't necessarily defined in $\mathbb{Z}[x]$, so we instead work in the field of fractions of $\mathbb{Z}[x]$, the smallest ring where polynomial division is defined. Then we proceed as follows:

$$\phi_p(x+1) = \frac{(x+1)^p - 1}{x+1-1} = \frac{x^p + \binom{p}{1}x^{p-1} + \cdots + \binom{p}{p-1}x + 1 - 1}{x} = x^{p-1} + px^{p-2} + \cdots + \binom{p}{2}x + p \in \mathbb{Z}[x].$$

This is an Eisenstein polynomial so it is irreducible.

□

3.4.14. Remark

These polynomials are called **cyclotomic polynoimals.**

3.4.15. Example

Consider $f(x) = x^3 - 3x - 1$.

3.4.16. ***Proposition:*** **Rational Root Test**

Let $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n \in \mathbb{Z}[x]$. Suppose that $f(m) \neq 0 \forall m$ such that $m \mid a_0$. Then f has no zeros in $\mathbb{Q}$.

Proof: Suppose by contradiction $\exists q = \frac{r}{s}$ such that $f(q) = 0$. We can assume $(r, s) = 1$ and $s \geq 1$.

Then $f(q) = 0 \Leftrightarrow a_0 + a_1\frac{r}{s} + \cdots + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \left(\frac{r}{s}\right)^n = 0$. Thus $r^n + a_{n-1}r^{n-1}s + \cdots + a_1rs^{n-1} + a_ns^n = 0$. So $r^n = -(a_{n-1}r^{n-1} + \cdots + a_1rs^{n-2} + a_0s^{n-1})s$. Since $(r, s) = 1$, we have $s = 1$. Then $f(r) = 0 \Rightarrow r^n + a_{n-1}r^{n-1} + \cdots + a_1r + a_0 = 0 \Rightarrow r(r^{n-1} + a_{n-1}r^{n-2} + \cdots + a_1) = -a_0$. So $r \mid a_0$, a contradiction.

□

3.4.17. ***Proposition***

Let R be a PID and let $f \in R$ be irreducible. Then (f) is a maximal ideal.

Proof: Suppose $\exists J \subseteq R$ is an ideal such that $(f) \subseteq J = (g)$, so $g \mid f$. So either $J = R$ or $J = (f)$ because f is irreducible.

□

3.4.18. ***Proposition***

Let K be a field and $R = K[X]$. We are interested in irreducible polynomials.

Let A be any PID and $a \neq 0$ in A. The following are equivalent

- a is irreducible
- (a) is a prime ideal
- (a) is a maximal ideal

Also, if a is irreducible, then $a \mid bc \implies a \mid b$ or $a \mid c$.

Proof:

□

3.5. Field Extensions

3.5.1. Definition: Field Extension

K' is a **field extension** of K if $K \subseteq K'$. If $\deg\left(\frac{K'}{K}\right) = \dim_K(K')$ is finite, then it is called a **finite field extension**.

3.5.2. *Corollary*

$f(x) \in K[x]$ is irreducible $\iff \frac{K[x]}{f(x)}$ is a finite field extension of K of degree $\deg(f)$. Furthermore, if f is irreducible, then K' is the smallest field extension of K which contains a root of $f(X)$.

Proof: It is clear from the previous proposition that $f(x)$ is irreducible $\iff K' = \left(\frac{K[x]}{f(x)}\right)$ is a field (because $K[X]$ is a PID). Look at $k \to K[x]$, $k \to \frac{k[x]}{(f(x))} = k'$, $k[x] \twoheadrightarrow \frac{k[x]}{f(x)} = k'$.

3.5.3. Remark

Recall that we saw that a field could be a vector space over itself. We can consider K' as a vector space over K and find a basis, as the following shows.

3.5.4. *Proposition*

Suppose $f(x)$ is irreducible. Consider $k \longrightarrow \frac{k[x]}{f(x)} = k'$. We claim that $\{1, \overline{x}, ..., \overline{x}^{n-1}\}$ is a K-basis of K' if $\deg(f) = n$ (note $\overline{x} = x \bmod f(x)$).

Proof: If $g(x) \in K[x]$, then $g(x) = q(x)f(x) + r(x)$ where $\deg(r(x)) < n$. Thus $g(x) \bmod f(x) = r(x) \bmod f(x)$. But $r(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \implies S$ generates K' as a K vector space. On the other hand, $a_n + a_{n-1}\overline{x} + \cdots + a_{n-1}\overline{x}^{n-1} = 0$ in K'. This implies $a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} = h(x)f(x) \in K[x]$. Thus $a_i = 0 \forall i \Rightarrow S$ is linearly independent.

□

Since $f(\overline{x}) = 0$ in K', we see that $\overline{x} \in K'$ is a root of $f(x)$. Suppose L is a field extension of K in which f has a root, say $a \in L$. Consider $\phi : K[x] \longrightarrow L$ defined by $\phi(x) = a$ (and ϕ is the identity on K). Since $f(a) = \phi(f) = 0$, this map uniquely factors as $k \hookrightarrow L$ and $k \hookrightarrow K'$ and $K' \hookrightarrow L$. So this is the smallest field in which it has a root.

□

3.5.5. Remark

The above shows why we care about irreducible polynomials. It is the condition we need to get a root, and many topics in math eventually boil down to doing that.

3.5.6. Example: Field of order 4

Consider $\mathbb{Z}_2[x]$ and $f(x) = x^2 + x + 1$. Observe this polynomial is irreducible by the Root Test. Consider $\frac{\mathbb{Z}_2[x]}{f(x)} = K'$ is a field extension of $\mathbb{Z}_2$ of degree 2, so $|K'| = 4$.

3.5.7. Example: Field of order 8

Consider $\mathbb{Z}_2[x]$ and $f(x) = x^3 + x + 1$. Observe it's again irreducible by the Root Test. Then $K' = \frac{\mathbb{Z}_2[x]}{f(x)}$ is a field extension of $\mathbb{Z}_2$ of degree 3. So $|K'| = 2^3 = 8$.

3.5.8. Example: Field of order 9

Consider $\mathbb{Z}_2[x]$ and $f(x) = x^2 + 1 \in \mathbb{Z}_3[x]$. Then $K' = \frac{K[x]}{f(x)}$ is a field extension of $\mathbb{Z}_3$ of degree 2, so $|K'| = 3^2 = 9$.

3.5.9. Remark

A natural question to ask is whether there exists a field of every prime power. It turns out there is, but constructing one is difficult and outside the scope of this class.

4. Important Classes of Rings

4.1. Euclidean Domains

4.1.1. Remark

Recall the ring of Gaussian integers $\mathbb{Z}[i]$, and how it had two copies of $\mathbb{Z}$. Recall $\mathbb{Z}$ was a PID, but what can we say about $\mathbb{Z}[i]$?

4.1.2. Definition: Euclidean Domain

Let R be an integral domain. We say that R is a **Euclidean domain** (ED) if $\exists$ a norm $N : R \to \mathbb{Z}$ (a function such that $N(0) = 0$) such that $\forall a, b \in R$ with $b \neq 0$, $\exists q, r \in R$ such that $a = qb + r$ with $r = 0 \vee N(r) < N(b)$.

4.1.3. Exercise

The norm is multiplicative.

Solution

4.1.4. Example

i) Every field is a Euclidean domain with respect to the trivial norm. If $a, b \in K$ and $b \neq 0$, $a = (b^{-1}a)b$.

ii) $R = \mathbb{Z}$ and $N(a) = |a|$, so $\mathbb{Z}$ is an ED.

iii) K is a field and $R = K[x]$. If $N(f(x)) = \deg(f(x))$, then R is a Euclidean domain by the division algorithm.

4.1.5. Example

People wondered whether a PID was also a Euclidean domain, but the following counterexample shows this is false. $x^2 + x + 5 \in \mathbb{Z}[x]$

Lecture 20 Feb 26

4.1.6. ***Theorem***

$\mathbb{Z}[i]$ is an ED.

Proof: $\mathbb{Z}[i] \subseteq \mathbb{C}$ and observe $N(a+bi) = |a+bi|^2 = a^2+b^2$. So $N(\alpha) = 0 \Leftrightarrow \alpha = 0$. If we take $\alpha = a+bi$ and $\beta = c+di \neq 0$, we get

$$\alpha\beta^{-1} = \frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{N(\beta)} = \frac{ac+bd}{N(\beta)} + \frac{bc-ad}{N(\beta)}i = r+si \in \mathbb{Q}[i].$$

Note we had to step out of $\mathbb{Z}[i]$ to get this to work.

Now by rounding, choose p and q such that $|r-p| \leq \frac{1}{2}$ and $|s-q| \leq \frac{1}{2}$. Then

$$\begin{aligned} \alpha\beta^{-1} &= r+si & &= (r-p+p)+(s-q+q) \\ &= [p+qi] + [(r-p)+(s-q)i] \\ &\implies \alpha = (p+qi)\beta + [(r-p)+(s-q)i]\beta \\ &\implies \alpha = t\beta + t' \end{aligned}$$

where $t = p+qi$ and $t' = [(r-p)+(s-q)i]\beta$. Now observe $t, \alpha, \beta \in \mathbb{Z}[i]$, which implies $t' \in \mathbb{Z}[i]$.

It remains to show $N(t') < N(\beta)$. Observe $N(t') = N(\beta)N((r-p)+(s-q)i)$. But $N((r-p)+(s-q)i) = (r-p)^2+(s-q)^2 \leq \frac{1}{4}+\frac{1}{4} = \frac{1}{2} \implies N(t') \leq \frac{N(\beta)}{2} < N(\beta)$.

□

4.1.7. Remark

We just saw that $\mathbb{Z}[i]$ is a Euclidean domain. Now what about $\mathbb{Z}[2i] = \{a+2bi : a, b \in \mathbb{Z}\}$?

It seems simple, but this is difficult question, since how can we know we can't find a norm? We must develop the theory further first.

4.1.8. ***Theorem***

Every Euclidean domain is a PID. (The converse is false due to Example above).

Proof: Let $I \subseteq R$ be an ideal. If $I = (0)$, there is nothing to prove. If $I \neq (0)$, there is an element $a \in I$ ($a \neq 0$) of smallest norm.

Let $b \in I$. Then we can find $q, r \in R$ such that $b = qa + r$ with $r = 0$ or $N(r) < N(a)$. If $r = 0$ we are done, and otherwise $r \in I$ and $N(r) < N(a)$, contradiction. Thus $a \mid b \Rightarrow I = (a)$.

□

4.1.9. Exercise

$\mathbb{Z}[2i]$ is generated by the ideal $I = (2, 2i)$, and is thus not an integral domain.

Solution

4.2. Unique Factorization Domains

4.2.1. Definition: Associate

If $a = ub$ with $u \in R^\times$, then a and b are **associates**.

4.2.2. Definition: Unique Factorization Domain (UFD)

Let R be an integral domain. We say that R is a **Unique Factorization Domain** if every nonzero element a which is not a unit has the following two properties:

i) a can be written as a finite product of irreducible elements, i.e., $a = p_1 \cdots p_n$ where p_i's are irreducible.
ii) This factorization of a is unique in the sense that if $a = q_1 \cdots q_m$ with q_i's irreducible, then $m = n$ and up to renumbering, q_i is an associate of p_i.

4.2.3. Example

i) Every field is a UFD (since every nonzero element is a unit, making it vacuously true).
ii) $R = \mathbb{Z}$
iii) What about $R = K[X]$? We will come back to this.
iv) $R = \mathbb{Z}[i]$ is an example.
iv) $R = \mathbb{Z}[2i]$ is not an example.

To see this, observe that $4 = 2 \cdot 2 = (2i)(-2i)$. We will show these elements are irreducible. Suppose $(a + 2bi)(a' + 2b'i) = 2 \implies (aa' - 4bb') + 2(ab' + a'b)i = 2$, so $aa' - 4bb' = 2 \Rightarrow 2 \mid aa'$, so either $2 \mid a$ or $2 \mid a'$. First suppose $2 \mid a \Leftrightarrow a = 2c$. Then we get $(2c + 2bi)(a' + 2b'i) = 2 \Rightarrow 2(c + bi)(a' + 2b'i) = 2 \Rightarrow (c + bi)(a' + 2b'i) = 1 \Rightarrow a' + 2b'i \in R^\times$.

Similarly, if $2 \mid a'$, then $a' + 2bi \in R^\times$, so 2 is irreducible.

4.2.4. ***Proposition***

$2 \in \mathbb{Z}[2i]$ is not a prime.

Proof:

$$\mathbb{Z}[2i] = \frac{\mathbb{Z}[x]}{x^2+4} \Rightarrow \frac{\mathbb{Z}[2i]}{(2)} = \frac{\mathbb{Z}_2[x]}{(x^2+4)} = \frac{\mathbb{Z}_2[x]}{(x^2)}$$

(where we just modded by 2 on both sides, and then observed 4 = 0 now).

This is not an integral domain since $x \cdot x = 0$, which shows 2 is not a prime by Proposition 2.3.3.

□

Lecture 21 Feb 28

4.2.5. ***Proposition***

Let R be a UFD. Let $a \in R$ be an irreducible element. Then a is a prime element. (Observe we have already proven this for a PID in 3.4.18)

Proof: Suppose $a \mid bc$. Write $b = p_1 \cdots p_n$ and $c = q_1 \cdots q_n$: products of irreducible elements. Since $a \mid bc$, write $bc = \alpha a$, so we can write $\alpha = r_1 \cdots r_s$, where each r_i is irreducible. Thus $bc = (r_1 \cdots r_s)a = (p_1 \cdots p_n)(q_1 \cdots q_m)$. By uniqueness of factorization of bc into irreducibles, we get that $a = up_i$ or $a = vq_j$ for some $u, v \in R^\times$. So $p_i = u^{-1}a$ and since $p_i \mid b$ we have $a \mid b$. Similarly, if the latter holds, then $a \mid c$.

□

4.2.6. ***Corollary***

$\mathbb{Z}[2i]$ is not a UFD.

Proof: This ring has irreducible elements which are not primes.

□

4.2.7. Definition: GCD

Let R be an integral domain. Let $a_1, ..., a_n \in R$. We say that $d = \gcd(a_1, ..., a_n)$ if
i) $d \mid a_i \forall i$
ii) $\forall c \in R, c \mid a_i \Longrightarrow c \mid d$

4.2.8. *Proposition*

Let R be a UFD and let $a, b \in R$ be nonzero elements. Then $\gcd(a, b)$ exists.

Proof: Choose irreducible elements $p_1, ..., p_n \in R$ such that $a = p_1^{e_1} \cdots p_n^{e_n}$ and $b = p_1^{f_1} \cdots p_n f^{f_n}$ where $a_i, f_i \geq 0$.

Let $g_i = \min(e_i, f_i)$ and write $d = p_1^{g_1} \cdots p_n^{g_n} \in R$. We claim that $d = \gcd(a, b)$. First, observe $d \mid a$ and $d \mid b$. Now suppose $c \mid a, b$. Write $c = q_1^{h_1} \cdots q_m^{h_m}$ as a unique factorization, so that $q_1^{h_1} \cdots q_m^{h_m} \mid p_1^{e_1} \cdots p_n^{e_n}$ and $q_1^{h_1} \cdots q_m^{h_m} \mid p_1^{f_1} \cdots p_n^{f_n}$. This means $q_1^{h_1} \mid p_1^{e_1} \cdots p_n^{e_n}$ and $q_1^{h_1} \mid p_1^{f_1} \cdots p_n^{f_n}$. Since q_1 is irreducible, it is prime by our previous proposition. Thus q_1 must be p_1 (after renumbering). So $q_1^{h_1} \mid p_1^{e_1}$ and $q_1^{h_1} \mid p_1^{f_1}$ so $q_1^m \mid p_1^{g_1}$. Similarly, $q_i^{h_i} \mid p_i^{g_i} \forall i$, so $c = q_1^{h_1} \cdots q_m^{h_m} \mid p_1^{g_1} \cdots p_n^{g_n} = d$.

□

4.2.9. *Proposition*

Let $a_1, ..., a_n \in R$ (an integral domain). Let $d \in (a_1, ..., a_n)$. Then $d = \gcd(a_1, ..., a_n) \iff (d) = (a_1, ..., a_n)$.

(Note if the gcd is not in the ideal, it doesn't work.)

Proof: Suppose that $d = \gcd(a_1, ..., a_n)$. Then $d \mid a_i \forall i \iff a_i \in (d) \forall i$. So $(a_1, ..., a_n) \subseteq (d) \subseteq (a_1, ..., a_n)$. Thus $(d) = (a_1, ..., a_n)$ so this is principal.

Conversely, suppose that $(d) = (a_1, ..., a_n)$. Then $a_i \in (d)$, so $d \mid a_i \forall i$. Let $c \in R$ such that $c \mid a_i \forall i$, so $a_i \in (c) \forall i$. Thus $(a_1, ..., a_n) \subseteq (c)$, but now $(d) \subseteq (c)$, so $c \mid d$. So $d = \gcd(a_1, ..., a_n)$.

□

4.2.10. Example

Consider $R = \mathbb{Z}[X]$ and take $a = p, b = x$ where p is prime. We claim $\gcd(p, X) = 1$. To see this, consider $\frac{R}{(p,X)} = \frac{\mathbb{Z}[X]}{(p,X)} = \mathbb{Z}_p$. Since $\mathbb{Z}_p$ is a field note that (p, X) is maximal, and we have shown previously that (p, X) is not principal. Observe $(p, X) \subseteq (\gcd(p, X))$ and since (p, X) is maximal and not principal, we must have $(\gcd(p, X)) = R$. Thus $\gcd(p, X)$ must be a unit, which we can take to be 1 (but since all units are associates any should work).

Lecture 22 — Mar 3

4.2.11. Definition: Ascending Chain of Ideals

An **ascending chain of ideals** (*) is a sequence of ideals $I_1 \subseteq I_2 \subseteq \cdots \subseteq \in R$. We say that (*) is stationary if $\exists N > 0$ such that $I_i = I_j \forall i, j \geq N$).

4.2.12. Definition: Noetherian Ring

Rings where every ascending chain of ideals is stationary are called **Noetherian**.

4.2.13. ***Proposition***

Let R be a commutative ring where every ideal is finitely generated. Then R is a Noetherian ring.

Proof: Let

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

be an ascending chain of ideals. Let $I := \bigcup_{i=1}^{\infty} I_i$; we claim this is an ideal.

Note that if $a, b \in I$ there must exist some $k \gg 0$ such that $a, b \in I_k$ implying that $a + b \in I_k \subseteq I$. Similarly, for $a \in I$ and $b \in R$ there exists some $j \gg 0$ such that $a \in I_j$ and therefore $ab \in I_j \subseteq I$. Therefore, I is an ideal and $I = \langle a_1, \ldots, a_r \rangle$.

This implies there exists some $n \gg 0$ such that $a_i \in I_n$ for any i. Therefore $I \subseteq I_n$ but $I_n \subseteq I$ such that $I = I_n$. Therefore $I_j = I_n$ for all $j \geq n$.

□

4.2.14. ***Corollary***

Let R be a PID. Then any ascending chain of ideals in R is stationary.

Proof: By the previous proposition, R is trivially a Noetherian ring, and therefore any ascending chain of ideals is stationary.

□

4.2.15. Example

$R = \mathbb{C}[0, 1]$. Define $\beta = \left[0, \frac{1}{n}\right]$ for $n \geq 1$. I.e., $I_n = \left\{ f \in R : f \mid_{\beta} = 0 \right\}$ is an ideal in R. Then $I_1 \subset I_2 \subset I_3 \subset \cdots$

Take any $n \geq 1$. Define

$$f(x) = \begin{cases} 0 \text{ if } 0 \leq x \leq \frac{1}{n+1} \\ x - \frac{1}{n+1} \text{ if } \frac{1}{n+1} \leq x \leq 1 \end{cases}$$

Thus $f \in I_{n+1} \setminus I_n$.

4.2.16. ***Theorem***

Every PID R is a UFD.

Proof: Let us first show that every nonzero nonunit element $a \in R$ has a factorization. Suppose a is irreducible. Then there's nothing to prove, so suppose it's reducible. Then we can write $a = a_1 a_2$ where neither a_1 nor a_2 is a unit. If a_1 and a_2 are irreducible, we are done. Otherwise, suppose a_1 is reducible. Then $a_1 = a_{11}a_{12}$, where neither is a unit. It remains to show that this process terminates.

Notice if it didn't stop, we get a chain of ideals

$$(a) \subset (a_1) \subset (a_{11}) \subset \cdots$$

4.2.17. ***Lemma***

If $a = a_1 a_2$ such that neither a_1 nor a_2 is a unit then $(a_1) \subsetneq (a)$.

Proof: Suppose to the contrary that $a_1 \in (a)$. Then we can write $a_1 = ab$ for some $b \in R$. So $a = a_1 a_2 = aba_2 \Rightarrow a - aba_2 = 0 \Rightarrow a(1 - ba_2) = 0 \Rightarrow ba_2 = 1 \Rightarrow a_2 \in R^\times$. Contradiction.

Observe this works in any integral domain, not necessarily a PID.

□

Now we show factorization is unique. Suppose $a = p_1 \cdots p_r = q_1 \cdots q_s \Rightarrow p_1 \mid q_1 \cdots q_s$. Since p_1 is irreducible and hence prime, $p_i \mid q_i$ for prime i. (Recall in a PID, irreducible implies prime).

Now we can assume without loss of generality $i = 1 \Rightarrow p_1 \mid q_1$. Since q_1 is irreducible, we must have that $q_1 = u_1 p_1$ for some $u_1 \in R^\times$. By induction on r and s, we must have $r - 1 = s - 1$ and q_j is an associate of p_j for $j \geq 2$. But then $r = s$ and $\forall i, q_i = u_i p_i$ for some $u_i \in R^\times$.

□

4.2.18. ***Corollary***

Let K be a field. Then $K[X]$ is a UFD.

Proof: We have shown that $K[X]$ is a PID.

□

4.2.19. *Corollary*

$\mathbb{Z}[i]$ is a UFD.

Proof: We showed that $\mathbb{Z}[i]$ is an ED. We also showed that ED $\Rightarrow$ PID.

□

4.2.20. Remark

Is $\mathbb{Z}[X]$ a UFD? We cannot yet answer this question, but this outlines our next goal.

We devise a trick to do this. Let R be a UFD. Let F be the field of fractions of R. This means $R[X] \hookrightarrow F[X]$. Now since we know $F[X]$ is a UFD, we observe that we might be able to use the map to go into $F[X]$, then come back to $R[X]$.

4.2.21. Definition: Least Common Multiple (LCM)

Let R be an integral domain. Let $a_1, ..., a_r \in R \setminus \{0\}$. Then an element $d \in R$ is called an lcm of $a_1, ..., a_r$ if
i) $a_i \mid d \forall i$
ii) $a_i \mid c \forall i$ for some $c \in R \implies d \mid c$

4.2.22. *Lemma*

Let $a_1, ..., a_r \in R$. Then lcm of $a_1, ..., a_r$ exists if and only if $\cap_{i=1}^{r} (a_i)$ is principal.

Proof: Suppose $\cap_{i=1}^{r} (a_i) = (d)$. Then $a_i \mid d \forall i$. If $a_i \mid c \forall i \implies c \in \cap (a_i) \Rightarrow d \mid c$.

Conversely, suppose $d = \text{lcm}(a_1, ..., a_r)$. Then $a_i \mid d \forall i \implies (d) \subseteq \cap (a_i)$. Also, if $c \in \cap (a_i) \Rightarrow a_i \mid c \forall i \Rightarrow d \mid c \forall i \Rightarrow c \in (d)$.

Thus $(d) = \cap (a_i)$.

□

4.2.23. *Corollary*

In a UFD, intersection of finitely many principal ideals is principal.

Proof:

□