35003 MODERN ALGEBRA

Prof Murray Elder, UTS

Week 7: rings, domains, fields, ideals, ring homomorphism

Lauritzen 3.1-3.3

RING

identity 0

Definition

A *ring* is an abelian group $(R, +)$ with an additional composition $\cdot : R \times R \to R$ called *multiplication*, which satisfies these axioms:

1. multiplication is associative: $\underline{(x \cdot y)}\ \underline{\cdot z} = x \cdot (y \cdot z)$ for all $x, y, z \in R$
2. there exists an element $1 \in R$ so that $1 \cdot x = x = x \cdot 1$ for all $x \in R$ (multiplicative identity)
3. distributive: $x \cdot (y + z) = x \cdot y + x \cdot z$ for all $x, y, z \in R$

RING

Definition

A *ring* is an abelian group $(R, +)$ with an additional composition $\cdot\colon R \times R \to R$ called *multiplication*, which satisfies these axioms:

1. multiplication is associative: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ for all $x, y, z \in R$
2. there exists an element $1 \in R$ so that $1 \cdot x = x = x \cdot 1$ for all $x \in R$ (multiplicative identity)
3. distributive: $x \cdot (y + z) = x \cdot y + x \cdot z$ for all $x, y, z \in R$

The neutral element of the abelian group $(R, +)$ is denoted 0.

RING

Definition

A *ring* is an abelian group $(R, +)$ with an additional composition $\cdot : R \times R \to R$ called *multiplication*, which satisfies these axioms:

1. multiplication is associative: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ for all $x, y, z \in R$
2. there exists an element $1 \in R$ so that $1 \cdot x = x = x \cdot 1$ for all $x \in R$ (multiplicative identity)
3. distributive: $x \cdot (y + z) = x \cdot y + x \cdot z$ for all $x, y, z \in R$

The neutral element of the abelian group $(R, +)$ is denoted 0.

Eg: $R = \mathbb{Z}$ with $+$ and multiplies.

Smaller: $\{0\}$ $0 \in R$ satisfies $0 \cdot 0 = 0$

2nd smaller $\{0, 1\}$ . . . ~~$(\mathbb{Z}/2\mathbb{Z}, +)$~~

RING

$(R, +, \cdot, 0, 1)$

Definition (3.1.1)

1. subring: S a subgroup of $\underline{(R, +)}$, $\underline{1 \in S}$ and $x, y \in S$ implies $x{}'y \in S$

RING

Definition (3.1.1)

1. subring: S a subgroup of $(R, +)$, $1 \in S$ and $x, y \in S$ implies $xy \in S$

2. $x \in R \setminus \{0\}$ is a *zero divisor* if $\exists y \in R \setminus \{0\}$ with $\underline{xy = 0}$ or $\underline{yx = 0}$

Check this is a ring $\left(\mathbb{Z}/6\mathbb{Z} ,\ \underset{\text{mod } 6}{+} ,\ \cdot \text{ mod } 6 \right)$

$2 \cdot 3 = 0$

~~not~~ zero divisor

RING

Definition (3.1.1)

1. subring: S a subgroup of $(R, +)$, $1 \in S$ and $x, y \in S$ implies $xy \in S$

2. $x \in R \setminus \{0\}$ is a *zero divisor* if $\exists y \in R \setminus \{0\}$ with $xy = 0$ or $yx = 0$

3. $x \in R$ is a *unit* if $\exists \underline{y} \in R$ with $xy = 1 = yx$.
   Ex:if x is a unit, the element y is unique.
   Then denote y as ~~y~~ x^{-1}. Set of units is $\underline{R^*}$

RING

Definition (3.1.1)

1. subring: S a subgroup of $(R, +)$, $1 \in S$ and $x, y \in S$ implies $xy \in S$

2. $x \in R \setminus \underline{\{0\}}$ is a *zero divisor* if $\exists y \in R \setminus \underline{\{0\}}$ with $xy = 0$ or $yx = 0$

3. $x \in R$ is a *unit* if $\exists y \in R$ with $xy = 1 = yx$.
   Ex:if x is a unit, the element y is unique.
   Then denote y as y^{-1}. Set of units is R^*

4. commutative if $\underline{xy = yx}$ for all $x, y \in R$

DEFINITIONS CONTINUED

eg $(\mathbb{Z}, +, \cdot, 0, 1)$

Definition

5. domain: no zero divisors

DEFINITIONS CONTINUED

Definition

5. domain: no zero divisors

6. field: every non-zero element is a unit; $R^* = R \setminus \{0\}$

DEFINITIONS CONTINUED

Definition

5. domain: no zero divisors

6. field: every non-zero element is a unit; $R^* = R \setminus \{0\}$

7. If $K \subseteq L$ are fields and K is a subring of L, we call K a *subfield* of L and call L and *extension field* of K.

DEFINITIONS CONTINUED

Definition

5. domain: no zero divisors
6. field: every non-zero element is a unit; $R^* = R \setminus \{0\}$
7. If $K \subseteq L$ are fields and K is a subring of L, we call K a *subfield* of L and call L and *extension field* of K.

Examples of fields: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$

So $\mathbb{Q}$ is a subfield of $\mathbb{R}$ and $\mathbb{C}$ is an extension field of $\mathbb{R}$.

EXAMPLES of rings.

1. $\mathrm{Mat}_2(\mathbb{R})$ $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ not commutative.

   has zero divisors

2. $\mathbb{C}$

3. Ring of quaternions $\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$ where $+$ is componentwise and multiplication is computed using the relations $i^2 = j^2 = k^2 = ijk = -1$.

   "non-commutative with a highly intricate multiplication"

EXAMPLES

1. $\mathrm{Mat}_2(\mathbb{R})$
2. $\mathbb{C}$
3. Ring of quaternions $\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$ where $+$ is componentwise and multiplication is computed using the relations $i^2 = j^2 = k^2 = ijk = -1$.

   "non-commutative with a highly intricate multiplication"

For the rest of Lauritzen, we only consider commutative rings.

PROPOSITIONS

Proposition (Prop 3.1.3)

Let R be a domain and $a, x, y \in R$. If $\underline{a \neq 0}$ and $\underline{ax = ay}$ then $x = y$.

Proof

$$ax = ay$$

$$ax - ay = 0$$

$$\|$$

$$a(x-y)$$

ay has additive inverse "$-ay$"

$a \neq 0$, R has no zero divisors,

$\therefore x - y = 0 \Rightarrow x = y$.

PROPOSITIONS

Proposition (Prop 3.1.3)

Let R be a domain and $a, x, y \in R$. If $a \neq 0$ and $ax = ay$ then $x = y$.

Proof: If $ax = ax$ then using the axioms of a ring, $ax - ay = 0$ and $a(x - y) = 0$. Since we are in a domain, a and $x - y$ are not zero divisors so we must have $x - y = 0$ (since $a \neq 0$ by assumption).

Thus $x = y$. $\square$

Proposition (Prop 3.1.4)

Every field F is a domain.

Direct F field $F^* = F \setminus \{0\}$ units.

Suppose $xy = 0$

If $x \neq 0$, $x \in F^*$ so has mult inverse

$y = 1 \cdot y = x^{-1} x y = x^{-1} 0 = 0$

$\therefore y = 0.$

$\therefore$ F has no zero divisors.

PROPOSITIONS

Proposition (Prop 3.1.4)

Every field F is a domain.

Proof: Let $x, y \in F$, $x \neq 0$ and $xy = 0$.

Since we are in a field there is an element $x^{-1} \in F$, so $y = x^{-1}xy = x^{-1}0 = 0$ by axioms of ring.

Thus x is not a zero divisor. □

PROPOSITIONS

Proposition (Prop 3.1.4)

Every field F is a domain.

Proof: Let $x, y \in F$, $x \neq 0$ and $xy = 0$.

Since we are in a field there is an element $x^{-1} \in F$, so $y = x^{-1}xy = x^{-1}0 = 0$ by axioms of ring.

Thus x is not a zero divisor. $\square$

Converse: $\mathbb{Z}$ is a domain, but not a field since $\mathbb{Z}^* = \{1, -1\}$.

EXAMPLE 3.1.5

Let $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$ be a subset of $\mathbb{C}$.

Ex: ($\mathbb{Q}(i)$ with the usual addition and multiplication of complex numbers) is a subring of $\mathbb{C}$.

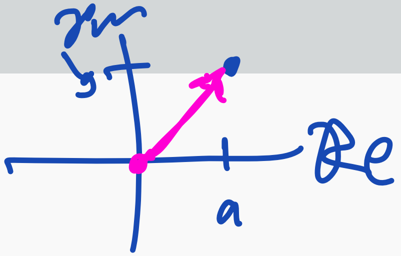
Ex: $\mathbb{Q}(i)$ is a field.

If $z = a + ib$ then $\frac{1}{z} = \frac{1}{a+ib} \frac{a \cancel{+} - ib}{a - ib}$ $\underline{\in \mathbb{Q}(i)}$

$$= \underset{\in \mathbb{Q}}{\frac{a}{a^2+b^2}} - \underset{\in \mathbb{Q}}{\frac{b}{a^2+b^2}}\, i$$

NORM

complex conjugate



in $\mathbb{C}$

Recall $\bar{z} = a - ib$ and $|z| = \sqrt{a^2 + b^2}$, and $|z|^2 = z\bar{z} = a^2 + b^2$.

Define $N(z) = |z|^2$ called the *norm* of z.

NORM

Recall $\bar{z} = a - ib$ and $|z| = \sqrt{a^2 + b^2}$, and $|z|^2 = z\bar{z} = a^2 + b^2$.

Define $N(z) = |z|^2$ called the *norm* of z.

Ex: $N(z_1 z_2) = N(z_1)N(z_2)$. in $\mathbb{C}$

Ex: if $z = a + ib$ with $a, b \in \mathbb{Z}$ then $\underset{\overset{\shortparallel}{a^2+b^2}}{N(z)} \in \mathbb{N}$. $= \{0, 1, 2, \dots\}$

GAUSSIAN INTEGERS

$\mathbb{Q}(i)$

$\mathbb{Z}[i]$.

Define $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ with the usual addition and multiplication in $\mathbb{Q}(i)$ and $\mathbb{C}$.

subring

This is a subring of $\mathbb{Q}(i)$ and called the *ring of Gaussian integers*.

GAUSSIAN INTEGERS

Define $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ with the usual addition and multiplication in $\mathbb{Q}(i)$ and $\mathbb{C}$.

This is a subring of $\mathbb{Q}(i)$ and called the *ring of Gaussian integers.*

What are the units of $\mathbb{Z}[i]$? (hint: use the norm) → $\mathbb{Z}[i]^* := \{1, -1, i, -i\}.$

Suppose $x \cdot y = 1$

$$N(xy) = N(1) = N(1 + 0i) = 1$$

$$N(xy) = \underline{N(x)}\,\underline{N(y)} \in \mathbb{N}$$

$\therefore N(x) = 1$

$a^2 + b^2 = 1$

$a = \pm 1$, $b = 0$ or $a = 0$, $b = \pm 1$

GAUSSIAN INTEGERS

Define $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ with the usual addition and multiplication in $\mathbb{Q}(i)$ and $\mathbb{C}$.

This is a subring of $\mathbb{Q}(i)$ and called the *ring of Gaussian integers.*

What are the units of $\mathbb{Z}[i]$? (hint: use the norm)

Since $N(z_1 z_2) = N(z_1)N(z_2)$, if $x, y \in \mathbb{Z}[i]$ and $xy = 1$ then $N(xy) = 1 = N(x)N(y)$ so the norm of a unit has to be (positive) 1.

Thus $a^2 + b^2 = 1$ only if $a = \pm 1$ or $b = \pm 1$, so

$$\mathbb{Z}[i]^* \subseteq \{\pm 1, \pm i\}.$$

To get $=$ check that each of these is a unit.

$\Rightarrow$ domain

Thus $\mathbb{Z}[i]$ is a domain (since it is a subring of the field $\mathbb{Q}(i)$) which is not a field.

$\mathbb{Z}[i]^* \neq \mathbb{Z}[i] \setminus \{0\}.$

GAUSSIAN INTEGERS

Thus $\mathbb{Z}[i]$ is a domain (since it is a subring of the field $\mathbb{Q}(i)$) which is not a field.

Are prime numbers still prime in $\mathbb{Z}[i]$?

Eg: $5 = (2+i)(2-i)$

IDEALS

$\forall x \in I$

A subset $I \subseteq R$ is an *ideal* in R if it is a subgroup of $(R, +)$ and $\lambda x \in I$ for every $\lambda \in R$.

Eg: $I = \{0\}$.

Ex: if $1 \in I$ then $R = I$.

$\lambda \cdot 1 \in I$ $\quad \forall \lambda \in R.$

IDEALS

A subset $I \subseteq R$ is an *ideal* in R if it is a subgroup of $(R, +)$ and $\lambda x \in I$ for every $\lambda \in R$.

Eg: $I = \{0\}$.

Ex: if $1 \in I$ then $R = I$.

Ex: If $I \subseteq F$ is an ideal in a field F, either $I = \{0\}$, or $x \in I$ for some $x \neq 0$, but then $\lambda = x^{-1}$ means

$$x^{-1} x = 1 \in I.$$

IDEAL GENERATED BY M

Ex: Let $r_1, \dots, r_n \in R$, then $\langle r_1, \dots, r_n \rangle = \underline{\{\lambda_1 r_1 + \cdots + \lambda_n r_n} \mid \lambda_i \in R\}$ is an ideal.

If I is an ideal that is equal to $\underline{\langle r_1, \dots, r_n \rangle}$ for some finite subset $\{r_1, \dots, r_n\} \subseteq R$ we say I is finitely generated.

IDEAL GENERATED BY M

Let $r_1, \ldots, r_n \in R$, then $\langle r_1, \ldots, r_n \rangle = \{\lambda_1 r_1 + \cdots + \lambda_n r_n \mid \lambda_i \in R\}$ is an ideal.

If I is an ideal that is equal to $\langle r_1, \ldots, r_n \rangle$ for some finite subset $\{r_1, \ldots, r_n\} \subseteq R$ we say I is finitely generated.

If M is any subset of R (finite or infinite) then
$\langle f \underset{\text{such that.}}{\mid} f \in M \rangle := \{$finite linear combinations of $f_i \in M\}$

$= \{\lambda_1 f_1 + \cdots + \lambda_n f_n \mid n \in \mathbb{N}, f_i \in M, \lambda_i \in R\}$

INTERSECTION, PLUS, PRODUCT

Ex: If $\underline{I, J}$ are ideals then so are

1. $\underline{I \cap} J$
2. $I + J = \{i + j \mid i \in I, j \in J\}$
3. $\underline{IJ = \langle ij \mid i \in I, j \in J \rangle}$. ideal generated by.

PID

If $I = \langle d \rangle$ for some $d \in R$ then I is called a Principal Ideal.

If D is a domain such that every ideal is a principal ideal, then D is called a Principal Ideal Domain (PID).

PID

ld

Suppose $x \in I$ x not multiple of d.

$x - qd \in I$

$\in I$ $\in I$ so $r \in I$

$x = qd + r$

$d > r > 0$

If $I = \langle d \rangle$ for some $d \in R$ then I is called a Principal Ideal.

If D is a domain such that every ideal is a principal ideal, then D is called a Principal Ideal Domain (PID).

Proposition (3.1.10)

$\mathbb{Z}$ is a PID.

$= \langle 0 \rangle$

Suppose I ideal in $\mathbb{Z}$. If $I \neq \{0\}$,

then $I \cap \mathbb{N}_+$ by well ordering principle

$\exists$ smaller element

$d \in I$ $d > 0$.

Z IS A PID

$\mathbb{Z}$ has no zero divisors so is a domain.

Every subgroup H of $(\mathbb{Z}, +)$ is either $\{0\}$ or has a smallest positive element, say d.

Then for every $n \in H$ we have $n = qd + r$ (well ordering principle; division algorithm: start of Chapter 1 Lauritzen)

$r = n - qd \in I.$

with $0 \leqslant r < d$. If $r \neq 0$ then d was not the smallest positive element of H.

So the only possible ideals in $\mathbb{Z}$ are of the form $d\mathbb{Z} = \langle d \rangle$ (since these are the only subgroups), and in fact they are ideals since $\lambda(dn) = d(\lambda n)$ for all $dn \in \langle d \rangle$. □

$\mathbb{Z}[i]$ IS A PID

Gaussian integers.

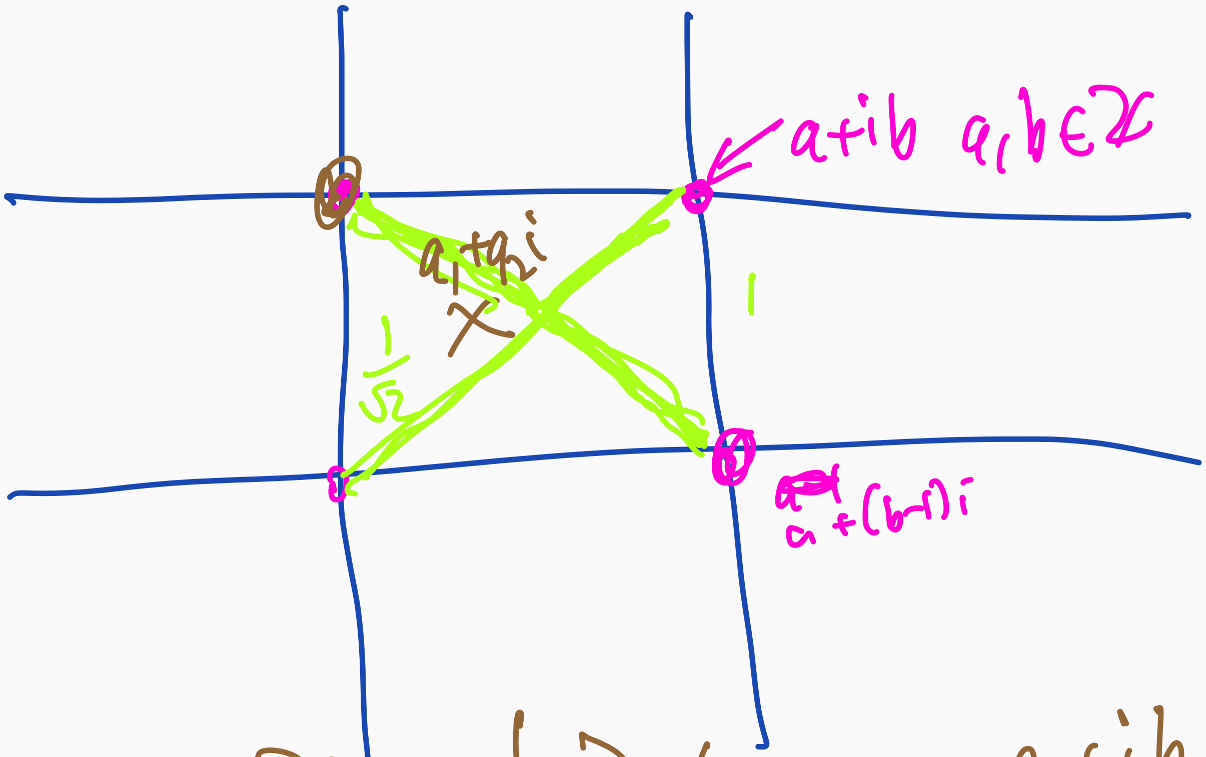
Let I be an ideal in $\mathbb{Z}[i]$ that is not $\{0\}$.

By the well ordering principle, the set $\{N(d) \mid 0 \neq d = a + ib \in \overset{I}{\mathbb{Z}[i]}\} \subseteq \mathbb{N}_+$ has a smallest value, so choose $0 \neq d \in I$ so that $N(d)$ is minimal.

Let $z \in I$, compute $z/d = q_1 + q_2 i$ where $q_i, q_2 \in \mathbb{Q}$.

$\mathbb{Q}(i)$.

$\mathbb{C}$



$$\exists\ a,b \in \mathbb{Z} \quad \left| z/d - a+ib \right| \leq \frac{1}{\sqrt{2}} < 1$$

$\mathbb{Z}[i]$ IS A PID

Let I be an ideal in $\mathbb{Z}[i]$ that is not $\{0\}$.

By the well ordering principle, the set $\{N(d) \mid 0 \neq d = a + ib \in \mathbb{Z}[i]\}$ has a smallest value, so choose $0 \neq d \in I$ so that $N(d)$ is minimal.

Let $z \in I$, compute $z/d = q_1 + q_2 i$ where $q_i, q_2 \in \mathbb{Q}$.

Draw lattice lines in the complex plane: any point is at most $\frac{1}{\sqrt{2}}$ away from a lattice point.

Z[i] IS A PID

Let I be an ideal in $\mathbb{Z}[i]$ that is not $\{0\}$.

By the well ordering principle, the set $\{N(d) \mid 0 \neq d = a + ib \in \mathbb{Z}[i]\}$ has a smallest value, so choose $0 \neq d \in I$ so that $N(d)$ is minimal.

Let $z \in I$, compute $z/d = q_1 + q_2 i$ where $q_i, q_2 \in \mathbb{Q}$.

Draw lattice lines in the complex plane: any point is at most $\frac{1}{\sqrt{2}}$ away from a lattice point.

Choose $x = \underline{c + id} \in \mathbb{Z}[i]$ to be a point within distance < 1 of z/d, so

$$|\underline{z/d} - x|^2 = N(\underbrace{z/d - x}_{\mathbb{Q}(i)}) < 1$$

$\mathbb{Z}[i]$ IS A PID

Let I be an ideal in $\mathbb{Z}[i]$ that is not $\{0\}$.

By the well ordering principle, the set $\{N(d) \mid 0 \neq d = a + ib \in \mathbb{Z}[i]\}$ has a smallest value, so choose $0 \neq d \in I$ so that $N(d)$ is minimal.

Let $z \in I$, compute $z/d = q_1 + q_2 i$ where $q_i, q_2 \in \mathbb{Q}$.

Draw lattice lines in the complex plane: any point is at most $\frac{1}{\sqrt{2}}$ away from a lattice point.

Choose $x = c + id \in \mathbb{Z}[i]$ to be a point within distance < 1 of z/d, so

$z \in I$

$-xd \in I$ $(x = d)$

$$|z/d - x|^2 = N(z/d - x) < 1$$

Multiply both sides by $N(d)$ (recall $N(pq) = N(p)N(q)$)

$$N(\overset{\in I}{z - xd}) = N(d)\, N\left(\frac{z}{d} - x\right) < N(d)$$

~~$N(d)$~~

Contradiction.

Z[i] IS A PID CONTINUED

$$N(d)N(z/d - x) < N(d)$$

$$N(z - xd) < N(d)$$

But $z \in I$, $d \in I$ and $\underline{x = \lambda \in} \mathbb{Z}[i]$ so $\underline{(z - xd) \in I}$ and has norm strictly smaller than $\underline{N(d)}$, so its norm has to be 0 by the choice of d.

$$N(z - xd) = 0$$

$$\therefore \quad z - xd = 0 \quad \cancel{\neq 0.}$$

$$z = xd \quad \rightarrow \in \langle d \rangle.$$

$\mathbb{Z}[i]$ IS A PID CONTINUED

$$N(d)N(z/d - x) < N(d)$$

$$N(z - xd) < N(d)$$

But $z \in I, d \in I$ and $x = \lambda \in \mathbb{Z}[i]$ so $(z - xd) \in I$ and has norm strictly smaller than $N(d)$, so its norm has to be $\underline{0}$ by the choice of d.

The only element of $\mathbb{Z}[i]$ with norm 0 is 0+0i, so $z = xd$ and $z \in \langle d \rangle$.

Thus $\underline{I \subseteq \langle d \rangle}$.

The other inclusion is clear since $d \in I$ means $\underline{\langle d \rangle} \subseteq \underline{I}$. □

WHAT ABOUT $\mathbb{Z}[\sqrt{-5}]$

Let $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$.

We have

$$\underline{6} = \underline{2.3} = \underline{(1+\sqrt{-5})(1-\sqrt{-5})}$$

Question: is $\underline{\langle 2, 1+\sqrt{-5}\rangle}$ a principal ideal?

QUOTIENT RING

Let I be an ideal of R.

So I is a subgroup of $(R, +)$ (abelian group) so I is automatically normal, and

$$R/I = \{x + I \mid x \in R\}$$

is a(n abelian) group (note we use additive notation here for the left cosets).

Let $[x] = x + I$. Then $[x] + [y] = (x + y) + I = [x + y]$.

We can make R/I into a ring by defining a multiplication and setting $1 + I$ to be the multiplicative identity:

$$[x] \cdot [y] = [xy]$$

Ex: check that addition and multiplication of left cosets does not depend on the choice of coset rep (is well defined) here is where we need I to be an ideal, not just a subgroup of $(R, +)$

NB: $[0] = 0 + I$ so $[x] = 0 \in R/I$ if and only if $x \in I$.

QUOTIENT RINGS OF Z

We proved the only ideals of $\mathbb{Z}$ are $d\mathbb{Z}$. A quotient ring of $\mathbb{Z}$ must therefore look like $\mathbb{Z}/I = \mathbb{Z}/d\mathbb{Z}$.

QUOTIENT RINGS OF Z

We proved the only ideals of $\mathbb{Z}$ are $d\mathbb{Z}$. A quotient ring of $\mathbb{Z}$ must therefore look like $\mathbb{Z}/I = \mathbb{Z}/d\mathbb{Z}$.

Aha, that's why Lauritzen writes the cyclic group of order d like that!!!

PROPOSITION 3.2.2

Proposition (3.2.2)

Let $d \in \mathbb{N}_+$. The group of units $(\mathbb{Z}/d\mathbb{Z})^*$ is an abelian group with $\varphi(d)$ elements (Euler's totient function, the number of $n \in \mathbb{N}^+$ with $\gcd(n, d) = 1$)

Proof: if $[x] = x + d\mathbb{Z}$ is a unit then $\exists \lambda \in R$ so that $[\lambda][x] = [1]$ so $\lambda x - 1 \in I = d\mathbb{Z}$, so $\lambda x - 1 = qd$ for some integers λ, q.

But

$$1 = \lambda x - qd$$

means if $c \in \mathbb{N}_+$ divides both x and d then c divides 1, so $\gcd(x, d) = 1$.

PROPOSITION 3.2.2

Proposition (3.2.2)

Let $d \in \mathbb{N}_+$. The group of units $(\mathbb{Z}/d\mathbb{Z})^*$ is an abelian group with $\varphi(d)$ elements (Euler's totient function, the number of $n \in \mathbb{N}^+$ with $\gcd(n, d) = 1$*)*

Proof: if $[x] = x + d\mathbb{Z}$ is a unit then $\exists \lambda \in R$ so that $[\lambda][x] = [1]$ so $\lambda x - 1 \in I = d\mathbb{Z}$, so $\lambda x - 1 = qd$ for some integers λ, q.

But

$$1 = \lambda x - qd$$

means if $c \in \mathbb{N}_+$ divides both x and d then c divides 1, so $\gcd(x, d) = 1$.

Conversely if $\gcd(x, d) = 1$ then by the Euclidean algorithm backwards we can find integers a, b so that $ax + bd = 1$. Then

$$[1] = [ax + bd] = [ax] + [bd] = [ax] + 0 = [a][x]$$

so $[x]$ is a unit and belongs to $(\mathbb{Z}/d\mathbb{Z})^*$. □

PROPOSITION 3.2.3

Proposition (3.2.3)

Let $n \in \mathbb{N}$.

Then $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is a prime.

If $n = 0$ then $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}$ is a domain.

If n is a composite number then $\mathbb{Z}/n\mathbb{Z}$ is not a domain.

Proof: Say $n > 0$.

By the previous result the size of the set of units is $\varphi(n)$ which equals $n - 1$ only when n is prime.

If $n = ab$ with $1 < a, b < n$ then $[a], [b]$ are not $[0]$ in $n\mathbb{Z}$, but $[a][b] = [n] = [0]$ so they are zero divisors. □

QUESTION

Let I be an ideal of R.

When is the quotient ring R/I a domain?

When is it a field?

If $R = \mathbb{Z}$ we can answer these, but more generally?

WHEN IS R/I A DOMAIN?

Suppose R/I is a domain (no zero divisors).

Then $R/I \neq \{[0]\}$ and for every $[x], [y] \in R/I$ if $[x][y] = [0]$ then one of $[x] = 0$ or $[y] = 0$.

Rephrasing this just in terms of the ideal I we have

$$I \neq R \quad \text{and} \quad \forall x, y \in R(xy \in I \text{ implies } x \in I \text{ or } y \in I)$$

WHEN IS R/I A DOMAIN?

Suppose R/I is a domain (no zero divisors).

Then $R/I \neq \{[0]\}$ and for every $[x], [y] \in R/I$ if $[x][y] = [0]$ then one of $[x] = 0$ or $[y] = 0$.

Rephrasing this just in terms of the ideal I we have

$$I \neq R \quad \text{and} \quad \forall x, y \in R(xy \in I \text{ implies } x \in I \text{ or } y \in I)$$

Definition: an ideal $I \in R$ is *prime* if it satisfies the previous line.

Ex: (3.21) $I \subset R$ is a prime ideal iff R/I is a domain.

WHEN IS R/I A FIELD?

Same idea for fields: come up with a condition on I that makes R/I a field.

WHEN IS R/I A FIELD?

Same idea for fields: come up with a condition on I that makes R/I a field.

Suppose R/I is a field.

(A field can be $\{[0]\}$ so Lauritzen typo here)

Being a field means every non-zero element (if there are any) have multiplicative inverses.

So every $[x] \in R/I$ has a $[y] \in R/I$ so that $[x][y] = [1]$.

WHEN IS R/I A FIELD?

In terms of the ideal I, we have: for every $x \notin I$ there exists $y \notin I$ so that $xy - 1 \in I$.

WHEN IS R/I A FIELD?

In terms of the ideal I, we have: for every $x \notin I$ there exists $y \notin I$ so that $xy - 1 \in I$.

Suppose that J is another ideal in between I and R, *i.e.* $I \subseteq J \subseteq R$.

If $x \in J \setminus I$ then we can find $y \notin I$ so that $xy - 1 \in I \subseteq J$ because of the above (assuming R/I is a field).

But since $x \in J$, $xy \in J$ because J is an ideal, and then $xy - 1 \in J$ means that $1 \in J$, and then $J = R$.

In other words, if R/I is a field, you cannot find any ideal $J \neq R$ that is bigger than I (contains I), because if there was you can choose $x \in J \setminus I$ and repeat the previous sentences.

WHEN IS R/I A FIELD?

Defn: An ideal $I \subseteq R$ is *maximal* if

$$I \subsetneq J \quad \text{implies} \quad J = R$$

WHEN IS R/I A FIELD?

Defn: An ideal $I \subseteq R$ is *maximal* if

$$I \subsetneq J \text{ implies } J = R$$

Ex: (Proposition 3.2.7) An ideal I is maximal if and only if R/I is a field.

We proved one direction of this on the previous slide (to come up with the defintion!)

WHEN IS R/I A FIELD?

Defn: An ideal $I \subseteq R$ is *maximal* if

$$I \subsetneq J \text{ implies } J = R$$

Ex: (Proposition 3.2.7) An ideal I is maximal if and only if R/I is a field.

We proved one direction of this on the previous slide (to come up with the defintion!)

NB: A maximal ideal means R/I is a field, which is a domain, which means I is a prime ideal.

That is, if I satisfies the condition to be maximal, then it satisfies the condition to be prime. (That would be a bit hard to prove from scratch)

RING HOMOMORPHISM

Definition

A map $f : R \to S$ between two rings R, S is a *ring homomorphism* if

- it is a group homomorphism from $(R, +)$ to $(S, +)$
- $f(xy) = f(x)f(y)$ for all $x, y \in R$
- $f(1) = 1$

RING HOMOMORPHISM

Definition

A map $f: R \to S$ between two rings R, S is a *ring homomorphism* if

- it is a group homomorphism from $(R, +)$ to $(S, +)$
- $f(xy) = f(x)f(y)$ for all $x, y \in R$
- $f(1) = 1$

If in addition f is a bijection, it is called a ring isomorphism, and we write $R \cong S$.

RING HOMOMORPHISM

Definition

A map $f : R \to S$ between two rings R, S is a *ring homomorphism* if

- it is a group homomorphism from $(R, +)$ to $(S, +)$
- $f(xy) = f(x)f(y)$ for all $x, y \in R$
- $f(1) = 1$

If in addition f is a bijection, it is called a ring isomorphism, and we write $R \cong S$.

$\ker(f) = \{x \in R \mid f(x) = 0\}$ as usual since f is a group homomorphism.

Ex: $\ker(f)$ is a ideal

ISOMORPHISM THEOREM FOR RINGS

Proposition (3.3.2)

Let R, S be rings, $f\colon R \to S$ a ring homomorphism. Then

$$\tilde{f}\colon R/\ker(f) \to f(R)$$

defined by $\tilde{f}(r + \ker(f)) = f(r)$ is a well-defined map and a ring isomorphism.

ISOMORPHISM THEOREM FOR RINGS

Proposition (3.3.2)

Let R, S be rings, $f\colon R \to S$ a ring homomorphism. Then

$$\tilde{f}\colon R/\ker(f) \to f(R)$$

defined by $\tilde{f}(r + \ker(f)) = f(r)$ is a well-defined map and a ring isomorphism.

Proof: by the Isomorphism theorem for groups, $\tilde{f}$ is a well-defined map and a group isomorphism, so we just have to check

- $\tilde{f}(1 + \ker(f)) = f(1) = 1$
- $\tilde{f}(x + \ker(f))\tilde{f}(y + \ker(f)) = f(x)f(y) = f(xy)$ since f is a ring homomorphism, and $\tilde{f}((x + \ker(f))(y + \ker(f))) = f(xy)$ by definition of $\tilde{f}$.

□

UNIQUE RING HOMOMORPHISM FROM Z

There is only one way we could define a map from $\mathbb{Z}$ to R so that it is a ring homomorphism:

$f(1) = 1$ and $f(1 + \cdots + 1) = f(1) + \cdots + f(1) = 1 + \cdots + 1$ means that $f(n)$ can only be this.

To check: the map $f : n \mapsto 1 + \cdots + 1$ (n times) is a ring homomorphism.

- it is clearly a group homomorphism from $(\mathbb{Z}, +)$ to $(R, +)$
- $f(1) = 1$ by construction
- $f(mn) = f(m)f(n)$:

UNIQUE RING HOMOMORPHISM FROM Z

There is only one way we could define a map from $\mathbb{Z}$ to R so that it is a ring homomorphism:

$f(1) = 1$ and $f(1 + \cdots + 1) = f(1) + \cdots + f(1) = 1 + \cdots + 1$ means that $f(n)$ can only be this.

To check: the map $f : n \mapsto 1 + \cdots + 1$ (n times) is a ring homomorphism.

- it is clearly a group homomorphism from $(\mathbb{Z}, +)$ to $(R, +)$
- $f(1) = 1$ by construction
- $f(mn) = f(m)f(n)$:

In light of this, it makes sense to think of integers as elements of any ring — when $n \in \mathbb{Z}$ we can write $n \in R$ to mean $1 + 1 + \cdots + 1$ (n times) is the element we are calling n

CHAR

Since $(R, +)$ is a group, the element $1 \in R$ has an order $\mathrm{ord}(1)$.

Definition

If $\mathrm{ord}(1)$ is infinite, we say R has *charactistic* zero.

Otherwise we say R has *charactistic* $\mathrm{ord}(1)$.

The characteristic of R is denoted $\mathrm{char} R$

The only time that $\mathrm{ord}(1) = 1$ is if $R = \{0\}$, otherwise $1 \neq 0$ and so $\mathrm{ord}(1) \geqslant 2$ in every other ring.

CHAR

Lemma (3.3.5)

Let R be a ring and $n = \mathrm{char} R$. Then there is an injective ring homomorphism $\mathbb{Z}/n\mathbb{Z} \to R$

Proof: Let $f : \mathbb{Z} \to R$ be the unique ring homomorphism. Then $f(\mathbb{Z})$ is a subring of R and $\ker(f) = ?$

which elements get sent to 0? $1 + \cdots + 1$ some multiple of $\mathrm{ord}(1) = \mathrm{char} R$ times by definition of char if $\mathrm{char} R > 0$ (and $(-1) + \cdots + (-1)$)

and if $\mathrm{char} R = 0$ then only 0 gets sent to 0 so $\ker(f) = \{0\}$.

CHAR

Lemma (3.3.5)

Let R be a ring and $n = \mathrm{char} R$. Then there is an injective ring homomorphism $\mathbb{Z}/n\mathbb{Z} \to R$

Proof: Let $f : \mathbb{Z} \to R$ be the unique ring homomorphism. Then $f(\mathbb{Z})$ is a subring of R and $\ker(f) =?$

which elements get sent to 0? $1 + \cdots + 1$ some multiple of $\mathrm{ord}(1) = \mathrm{char} R$ times by definition of char if $\mathrm{char} R > 0$ (and $(-1) + \cdots + (-1)$)

and if $\mathrm{char} R = 0$ then only 0 gets sent to 0 so $\ker(f) = \{0\}$.

The isomorphism theorem for rings says that $\tilde{f}$ is an isomorphism onto $f(\mathbb{Z}) \subseteq R$, so it is an injective homomorphism to R. □

CHAR FOR DOMAINS

Proposition (Prop 3.3.7)

Let R be a domain. Then $\mathrm{char} R$ is either 0 or a prime. If R is finite then R is a field and $\mathrm{char} R$ is a prime number.

CHAR FOR DOMAINS

Proposition (Prop 3.3.7)

Let R be a domain. Then $\mathrm{char} R$ is either 0 or a prime. If R is finite then R is a field and $\mathrm{char} R$ is a prime number.

Proof: Let $n = \mathrm{char} R$. By the previous result we have $\mathbb{Z}/n\mathbb{Z}$ sitting inside R (the image of $\mathbb{Z}/n\mathbb{Z}$ under $\tilde{f}$ at least).

Since R is a domain, $\tilde{f}(\mathbb{Z}/n\mathbb{Z})$ must be a domain since its a subring, and it is isomorphic to $\mathbb{Z}/n\mathbb{Z}$, so the only way that can be a domain is if n is prime or 0.

CHAR FOR DOMAINS

Proposition (Prop 3.3.7)

Let R be a domain. Then $\mathrm{char}R$ is either 0 or a prime. If R is finite then R is a field and $\mathrm{char}R$ is a prime number.

Proof: Let $n = \mathrm{char}R$. By the previous result we have $\mathbb{Z}/n\mathbb{Z}$ sitting inside R (the image of $\mathbb{Z}/n\mathbb{Z}$ under $\tilde{f}$ at least).

Since R is a domain, $\tilde{f}(\mathbb{Z}/n\mathbb{Z})$ must be a domain since its a subring, and it is isomorphic to $\mathbb{Z}/n\mathbb{Z}$, so the only way that can be a domain is if n is prime or 0.

If R is a finite domain it cannot contain $\mathbb{Z}$ so it must be prime characteristic.

Worksheet exercise (first one) we showed a finite domain is a field. □

UNDERGRAD'S DREAM

Theorem (3.3.9)

Let R be a ring of prime characteristic. Then

$$(x+y)^{p^r} = x^{p^r} + y^{p^r}$$

✓

for all $x, y \in R$ and $r \in \mathbb{N}$.

UNDERGRAD'S DREAM

Theorem (3.3.9)

Let R be a ring of prime characteristic. Then

$$(x+y)^{p^r} = x^{p^r} + y^{p^r}$$

for all $x, y \in R$ and $r \in \mathbb{N}$.

Proof: Let $\mathrm{char} R = p$ prime.

First prove the binomial theorem in the setting of a ring:

$$\boxed{(a+b)^n = a^n + \binom{n}{1} a^{n-1} b + \cdots + \binom{n}{n-1} a b^{n-1} + b^n}$$

which makes since since $\mathbb{Z}$ lives inside any ring R.

Prove by induction and the combinatorial identity (of numbers)

$$\binom{n}{i} + \binom{n}{i-1} = \binom{n+1}{i}$$

undergrad's dream proof continued

Second, you need to prove that p divides $\binom{p}{i}$ for $1 \leqslant i \leqslant p-1$.

(Use the fact that if $p \mid ab$ then $p \mid a$ or $p \mid b$ for any $a, b \in \mathbb{Z}$)

UNDERGRAD'S DREAM PROOF CONTINUED

Second, you need to prove that p divides $\binom{p}{i}$ for $1 \leqslant i \leqslant p-1$.

(Use the fact that if $p \mid ab$ then $p \mid a$ or $p \mid b$ for any $a, b \in \mathbb{Z}$)

Then since we are in a ring of characteristic p, $1 + \cdots + 1$ (p times) equals 0, so all of the middle terms of the binomial expansion disappear:

$$(x+y)^p = x^p + y^p$$

Finally, by induction (base case done) we have

$$(x+y)^{p^r} = ((x+y)^p)^{p^{r-1}} = ((x^p + y^p)^{p^{r-1}}$$

$$= ((x^p)^{p^{r-1}} + ((y^p)^{p^{r-1}}$$

□

NEXT:

Friday: workshop doing Lauritzen 3.6 exercises

Next week: assessment 2

After StuVac:

Freshman's dream.

- Week 9: Undergrad's dream; field of fractions; UFD (and the answer to the mystery of whether $\mathbb{Z}[\sqrt{-5}]$ is a PID)
- Week 10: Polynomial rings. Seminar report due this week.
- Week 11: more polynomial rings (sketch of classification of finite fields)
- Week 12: final assessment (1B)