Lecture 3

$\mathbb{Q}[\sqrt{2}] \subset \mathbb{R}$, $\quad \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ $\quad \Rightarrow a = a', b = b'$

$a + b\sqrt{2} = a' + b'\sqrt{2}$

Prop $\mathbb{Q}[\sqrt{2}]$ is a field.

Proof (a) $\mathbb{Q}[\sqrt{2}]$ is a subring of $\mathbb{R}$ $\Rightarrow$ $\mathbb{Q}[\sqrt{2}]$ is a commutative ring

$$(a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{2}$$

$$(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = (a_1 a_2 + 2b_1 b_2) + (a_1 b_2 + a_2 b_1)\sqrt{2}$$

(b) To construct the inverse of $a + b\sqrt{2}$

$$(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$$

similar to conjugate of a complex number

rational number.

$\Rightarrow$

$$(a + b\sqrt{2})^{-1} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}$$

defined unless $a = b = 0$.

$\Rightarrow$ $\mathbb{Q}[\sqrt{2}]$ is a field.

Lemma: $a^2 - 2b^2 = 0$ for rational a, b iff $a = b = 0$.

Proof: by analogy with same statement for integral a, b.

$a = \frac{n_1}{m_1}$, $b = \frac{n_2}{m_2}$

$a^2 = 2b^2 \Rightarrow \frac{n_1^2}{m_1^2} = 2\frac{n_2^2}{m_2^2} \Rightarrow$

$n_1^2 m_2^2 = 2 m_1^2 n_2^2$

$(n_1 m_2)^2 = 2(m_1 n_2)^2$

reduce to integral case.

$n_1 = 2n_3$

Other examples

$\mathbb{Q}[\sqrt{n}] \subset \mathbb{R}$ a subfield. $\quad \mathbb{Q}[\sqrt{n}] \neq \mathbb{Q}$ if n is not a perfect square

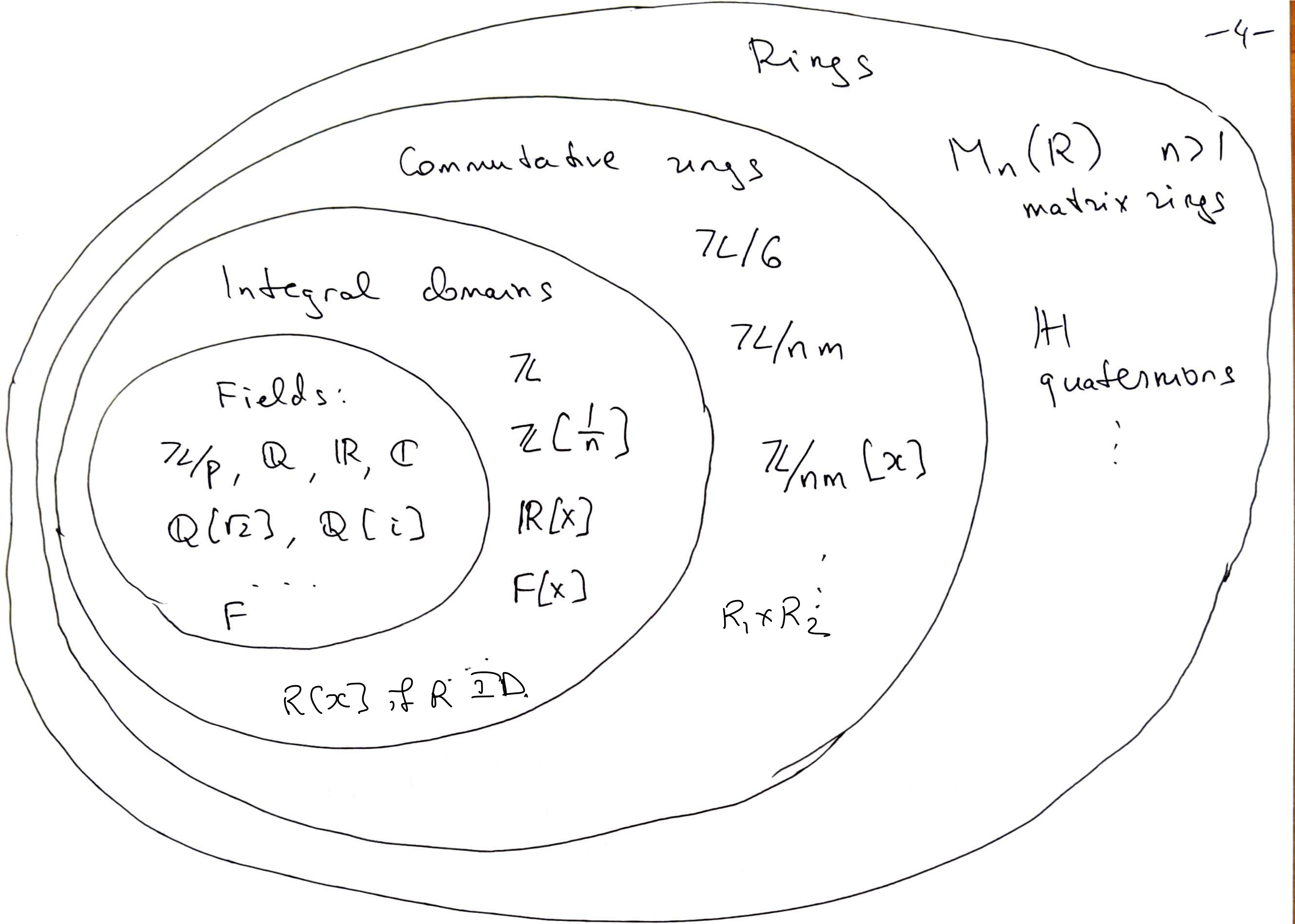
$\mathbb{Z}[\sqrt{n}] \subset \mathbb{R}$ a subring, not a ~~subfi~~ field.

$\mathbb{Q}[i] \subset \mathbb{C}$ a field (Gaussian rationals) $\quad \mathbb{Q}[i] = \{a + bi \mid a, b \in \mathbb{Q}\}$

$(a + bi)(a - bi) = a^2 + b^2 \neq 0$ $\quad$ usual inverse $(a + bi)^{-1} = \frac{a - bi}{a^2 + b^2} = \underbrace{\frac{a}{a^2 + b^2}}_{\in \mathbb{Q}} - \underbrace{\frac{b}{a^2 + b^2}}_{\in \mathbb{Q}} i$

$\mathbb{Q}[\sqrt{n}]$, $\mathbb{Q}[i]$ - subfields of $\mathbb{R}$ and $\mathbb{C}$, respectively

$\mathbb{Z}[i] \subset \mathbb{Q}[i]$ - ring of Gaussian integers, $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$



R is an ID $\quad\quad\quad\quad\quad\quad\quad\quad$ $R[x]$

<u>Theorem</u> If F is a field, the ring of polynomials $F[x]$ is an integral domain.

<u>Lemma</u>: if $f(x), g(x) \in F[x]$, $\deg(fg) = \deg(f) + \deg(g)$

Pf: $f = \sum_{i=1}^{n} a_i x^i$, $g = \sum_{j=1}^{m} b_j x^j$ $\quad \deg f = n$, $\deg g = m$ $\quad a_n \neq 0$, $b_m \neq 0$

$\Downarrow$

$f(x)\cdot g(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \dots + a_n b_m x^{n+m}$ $\quad a_n b_m \neq 0$

$\Rightarrow a_n b_m \neq 0$, $\deg(fg) = n+m$

$\Rightarrow$ if $f(x)g(x) = 0$ need <u>top</u> nonzero coefficient of f or g to be 0 $\Rightarrow f = 0$ or $g = 0$.

lemma holds for F an integral domain, in general

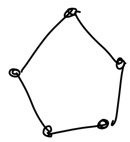
$f = a_0 \neq 0$ $\quad \deg f = 0$

$f = a_0 + a_1 x$, $a_1 \neq 0$ $\quad \deg f = 1$

convention: $f = 0$ $\quad \deg(0) = -\infty$

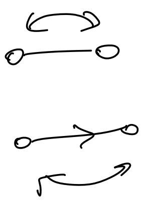
$S_n = Sym(\{1, \dots, n\})$

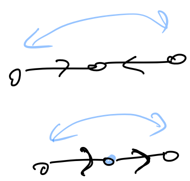
<u>graphs</u>

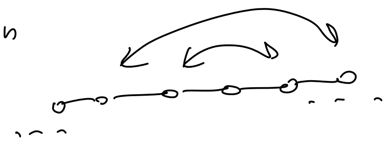


D_n

C_n







S b)

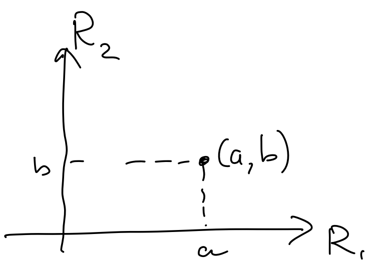
Direct products $\quad R_1 \times R_2 = \{(a,b) \mid a \in R_1, b \in R_2\}$

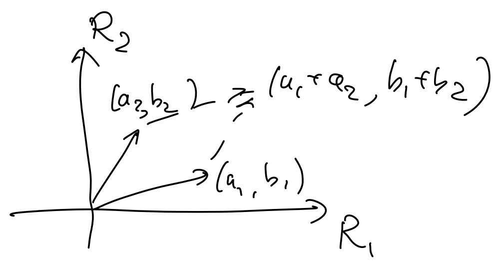
$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$

$(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2)$

$(1,1)(a,b) = (a,b)$ $\qquad 1 = (1,1)$

$(0,0)$ $\qquad 0 = (0,0)$





<u>Prop</u> there are homomorphisms

$$R_1 \times R_2 \longrightarrow R_1$$
$$(a, b) \longmapsto a$$

forget b. $\qquad (1,1) \longmapsto 1$

<u>Ex</u> this is a homomorphism

$$R_1 \times R_2 \longrightarrow R_2$$
$$(a, b) \longmapsto b$$

$R_1 \longrightarrow R_1 \times R_2$

$1 \longmapsto (1, 0)$

$a \longmapsto (a, 0)$

$R_2 \longrightarrow R_1 \times R_2$

$b \longmapsto (0, b)$

don't take 1 to 1

respects $+, \cdot$

non-unital homomorphism

Idempotent is an element $e \in R$ such that $e^2 = e$.

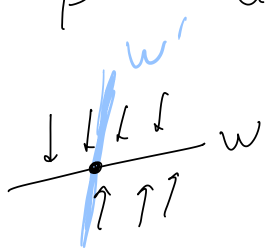
$\forall$ ring has idempotents $1, 0$ $\quad 1^2 = 1,\ 0^2 = 0$

$(1,0)^2 = (1^2, 0^2) = (1,0)$

$(0,1)^2 = (0,1)$

$M_n(\mathbb{R})$ has many idempotents.

P lin. operator $\quad P^2 = P$



$P_W \quad V = \mathbb{R}^n$

$W + W' = V$

$W \cap W' = \{0\}$

$V = W \oplus W'$

project onto W, send W' to 0

$P_V(v) = w$

$v = (w, w')$

$v = \underset{W}{w} + \underset{W'}{w'}$

idempotent or projector

idempotent are noninvertible (except for 1)

$e: R \longrightarrow R$

$e: a \longmapsto ea$

$\mathbb{Z}/6 \quad 0, 1 \quad 3^2 = 3 \pmod 6$

idempotent

$4^2 = 16 \equiv 4 \pmod 6$

$3+4 \equiv 1 \pmod 6$ complementary idempotent

e idempotent $\rightarrow$ $1-e$ idempotent (exercise)

$(1-e)^2 = 1-2e+e^2 = 1-e$

$(a-b)^2 = a^2 - ab - ba + b^2$ $\quad e(1-e) = 0$

$(1-e)e = 0$

orthogonal idempotents.

$R_1 \times R_2 \qquad (1,1) = (1,0) + (0,1)$

$3^2 = 3$

$\mathbb{Z}/6 \simeq \mathbb{Z}/2 \times \mathbb{Z}/3 \qquad \mathbb{Z}/2 \ \{0,3\}$

$0,1 \qquad 0,1,2 \qquad \mathbb{Z}/3 \ \{0,2,4\}$

$\{0,2 \ 1\}$

$0 \leftarrow (0,0)$

$3 \leftarrow (1,0)$

$4 \leftarrow (0,1)$

$1 \leftarrow (1,1)$

$2 \leftarrow (0,2)$

$5 \leftarrow (1,2)$

$\gcd(n,m) = 1$

$(n,m) = 1$

Thm if $\gcd(n,m)=1 \Rightarrow$

$\mathbb{Z}/nm \simeq \mathbb{Z}/n \times \mathbb{Z}/m$

Assume all rings are commutative unless otherwise specified.

Def $r \in R, r \neq 0$ is called a zerodivisor if $\exists s \in R, s \neq 0$ s.t. $rs = 0$

$\mathbb{Z}/nm$

n,m zero divisors

$R = \mathbb{Z}/6[x]$

$(2x)(3x) = 6x^2 = 0$

Def Ring R is an <u>integral domain</u> if the product of two non-zero elements in R is itself nonzero.

R is an integral domain $\Leftrightarrow$ it has no zero divisors.
ID

1) $\mathbb{Z}$ is an ID
2) $\forall$ field F is an ID. $\quad r \quad r^{-1}$

$rs = 0 \qquad r^{-1}(rs) = r^{-1} \cdot 0$

$s = 0$

3) $S \subset R$ (subring), R an ID $\Rightarrow$ S is an ID.

<u>Corollary</u> Any subring of a field $(\mathbb{R}, \mathbb{C}, \ldots)$ is an integral domain

$\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[i]$

$R_1 \times R_2$ <u>not</u> ID $\qquad (1,0)(0,1) = (0,0) = 0$

$\mathbb{Z}[x,y] / xy = 0 \qquad$ generators & relations

group G $\quad a, b \qquad a^2bab^2a^3 = 1$

$bab^{-1}ab^{-1}a = 1$

<u>Thm</u> A ring R is an ID iff it satisfied the <u>cancellation law</u>:

if $ra = rb$ and $r \neq 0$ then $a = b$

<u>Proof</u> $\quad ra = rb \Leftrightarrow r(a-b) = 0 \qquad \cancel{r}a = \cancel{r}b$

$\Rightarrow$ If R is an ID $\Rightarrow r$ <u>not</u> a zero divisor $\Rightarrow$

$a-b=0$, $a=b$.

$\Leftarrow$ if cancellation law holds in R,

if $ab=0$, $a,b\neq 0$ $\quad ab=0=0\cdot b$

$a\cancel{b}=0\cdot\cancel{b}$ $\quad a=0$

$\mathbb{Z}/6$ $\quad \cancel{3}\cdot 2=\cancel{3}\cdot 4 \Rightarrow 2=4$ false.

<u>Thm</u> $\mathbb{Z}/n$ is an ID iff n is prime.

$\Rightarrow$ if $n=ab \Rightarrow a\cdot b\equiv 0 \pmod n$ $\quad a,b\not\equiv 0 \pmod n$

not an ID.

$\Leftarrow$ $n=p$ $\quad ab\equiv 0 \pmod p \Rightarrow p|a$ or $p|b \Rightarrow a\equiv 0$ or $b\equiv 0 \pmod p$.

<u>Thm</u> $\mathbb{Z}/n$ is a field iff n is prime.

$n=p$ prime

$0<a<p$

$(a,p)=1$

$\exists s,t$ $\quad sa+tp=1$ $\quad s=a^{-1} \pmod p$

$sa\equiv 1 \pmod p$ $\quad tp\equiv 0 \pmod p$

<u>lemma</u> $(a,b)=1 \Leftrightarrow$

$\exists s,t$ $\quad sa+tb=1$.

Int. Dom $\quad$ field

$\mathbb{Z} \longrightarrow \mathbb{Q}$

$n \longmapsto \frac{1}{n}$

Can invert $\underbrace{\text{el's}}_{\text{nonzero}}$ of any ID to get a field

ID

$R \rightsquigarrow F=\mathrm{Frac}(R)$

f. fractions of R.

if R has zero div

$rs=0$, $r\neq 0$, $s\neq 0$

$\frac{1}{r}\cdot\frac{1}{s}=\frac{1}{rs}=\frac{1}{0}$

$\frac{a}{b}$, $b \neq 0$ $\qquad \frac{a\cancel{c}}{b\cancel{c}} = \frac{a}{b}$, $c \neq 0$ $\qquad \frac{a}{b} = \frac{c}{d}$ if $ad = bc$

Consider set of pairs $\{(a,b) \mid a, b \in R,\ b \neq 0\} = S$

Equivalence relation on S $\sim$

$(a,b) \sim (c,d)$ iff $ad = bc$ $\qquad \frac{a}{b}$

<u>lemma</u> $\sim$ is an equivalence relation

$(a,b) \sim (a,b)$; $\quad (a,b) \sim (c,d) \Leftrightarrow (c,d) \sim (a,b)$

$(a,b) \sim (c,d)$, $(c,d) \sim (e,f)$ $\quad$ want $(a,b) \sim (e,f)$

$ad = bc \qquad cf = de \qquad af = be$

mult f $\qquad$ mult b

$$adf = bcf = deb$$

$$a\cancel{d}f = \cancel{d}eb$$
$$af = eb$$

$$\mathrm{Frac}(R) = S/\sim$$

define addition, $\qquad (a,b)$ write as $\frac{a}{b}$, $b \neq 0$

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \qquad bd \neq 0$$

need to check well-defined

$\frac{a}{b} \sim \frac{a'}{b'} \Leftrightarrow ab' = a'b$ $\quad$ want $\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c}{d}$

$$\frac{ad+bc}{bd} \sim \frac{a'd+b'c}{b'd}$$

$(ad+bc)\,b'd \overset{?}{=} (a'd+b'c)\,bd$ given $ab' = a'b$

$$adb'd + \cancel{bcb'd} \overset{?}{=} a'dbd + \cancel{b'cbd}$$

$$adb'd \stackrel{?}{=} a'dbd$$

$$ab'd^2 \stackrel{?}{=} a'bd^2 \Leftarrow ab' = a'b$$

$+$ is well-defined. $\frac{a}{b}$

$\cdot$ is well-defined.

$(0,1) \sim (0,b)$ $\quad b \neq 0$ $\qquad 0 = (0,1)$

$\frac{0}{1} + \frac{a}{b} = \frac{a}{b}$ (exercise)

$-(a,b) = (-a,b)$

1) Check that $S/\sim = \mathrm{Frac}(R)$ is an abelian group under addition.

2) $(1,1)$ $\frac{1}{1}$

$\sim (a,a)$ $a \neq 0$

3) $\cdot$ is well-defined, assoc.

4) distributivity

<u>Thm</u> $\mathrm{Frac}(R)$ is a field that contains R as a subring.

$$R \to \mathrm{Frac}(R)$$

$$a \mapsto (a,1) \quad \frac{a}{1}$$