Lecture 3

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

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.

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, $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$

From now on, all rings are commutative, unless specified otherwise.

Def $r \in R$, $r \neq 0$ is called a zero divisor if there exist $s \in R$, $s \neq 0$ such that $rs = 0$.

(Note that s is also a zero divisor then)

Example 1) $R = \mathbb{Z}/6$ $\quad 2 \cdot 3 = 0 \quad 2 \neq 0, 3 \neq 0 \Rightarrow 2, 3$ are zero divisors in $\mathbb{Z}/6$

2) $R = \mathbb{Z}/nm$ $\quad n \circ m = 0 \quad n, m \neq 0 \Rightarrow n, m$ are zero divisors in $\mathbb{Z}/nm$

3) $R = \mathbb{Z}/6[x]$ $\quad 2x$ is a zero divisor $\quad 2x \cdot 3 = 6x = 0 \cdot x = 0$

$2x \neq 0$ in R

Remark: Rotman uses $[k]$ to denote $k \pmod{n}$ $\quad [2][3] = [6] = 0$ in $\mathbb{Z}/6$.

(also uses $\mathbb{Z}_6$ instead of $\mathbb{Z}/6$)

Def Ring R is an integral domain (or just domain) if the product of two nonzero elements in R is itself nonzero.

R is an integral domain iff it has no zero divisors.

Examples 1) $\mathbb{Z}$ is an integral domain

2) Field F is an integral domain: an invertible element r cannot be a zero divisor: $\quad rr^{-1} = 1$; if $rs = 0$ multiply by r^{-1}

$r^{-1}(rs) = r^{-1} \cdot 0 \Rightarrow r^{-1}rs = r^{-1} \cdot 0 \Rightarrow s = 0$.

3) Exercise: If $S \subset R$ is a subring and R is an integral domain then S is an integral domain

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

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

Theorem A ring R is an integral domain iff it satisfies the cancellation law: if $ra = rb$ and $r \neq 0$ then $a = b$

Proof: $ra = rb \iff \underbrace{r(a-b) = 0}_{(r=0 \text{ or } a-b=0)}$.

If R is an integral domain $\Rightarrow r$ is not a zero divisor $\Rightarrow a-b=0$, $a=b$.

If cancellation law holds in R. If $\exists r, a \in R$, $r, a \neq 0$ with $ra = 0$. $\Rightarrow$

$ra = 0 = r \cdot 0$. Can cancel r from $ra = r0 \Rightarrow a = 0$ contradiction

Example $R = \mathbb{Z}/6$ $\quad 3 \cdot 2 = 3 \cdot 4$ since $6 = 12 \pmod 6$. But cannot cancel 3: $3 \neq 0$

$\cancel{3} \cdot 2 = \cancel{3} \cdot 4 \quad 2 = 4$ wrong

Thm $\mathbb{Z}/n$ is an integral domain iff n is prime

Proof If n is composite, $n = ab$, $1 < a < n$, $1 < b < n \Rightarrow a, b$ are zero divisors in $\mathbb{Z}/n$ $\quad a \neq 0, b \neq 0 \quad ab = n \equiv 0 \pmod n$

If $n = p$ - prime. Assume $ab \equiv 0 \pmod p$. Then p divides ab $\Rightarrow p$ divides a or b (Euclid's lemma) $\Rightarrow a \equiv 0 \pmod p$ or $b \equiv 0 \pmod p$ $\Rightarrow a = 0$ in $\mathbb{Z}/p$ or $b = 0$ in $\mathbb{Z}/p$ (Rotman writes $[a]$ for $a + n\mathbb{Z}$, etc.)

$\Rightarrow \mathbb{Z}/p$ is an integral domain. Even better:

Thm $\mathbb{Z}/p$ is a field, for any prime p.

Proof Let $[a] \in \mathbb{Z}/p$. If $[a] \neq 0$ in $\mathbb{Z}/p$, then p does not divide a. Since p is prime, $\gcd(a, p) = 1$ (greatest common divisor of a and p)

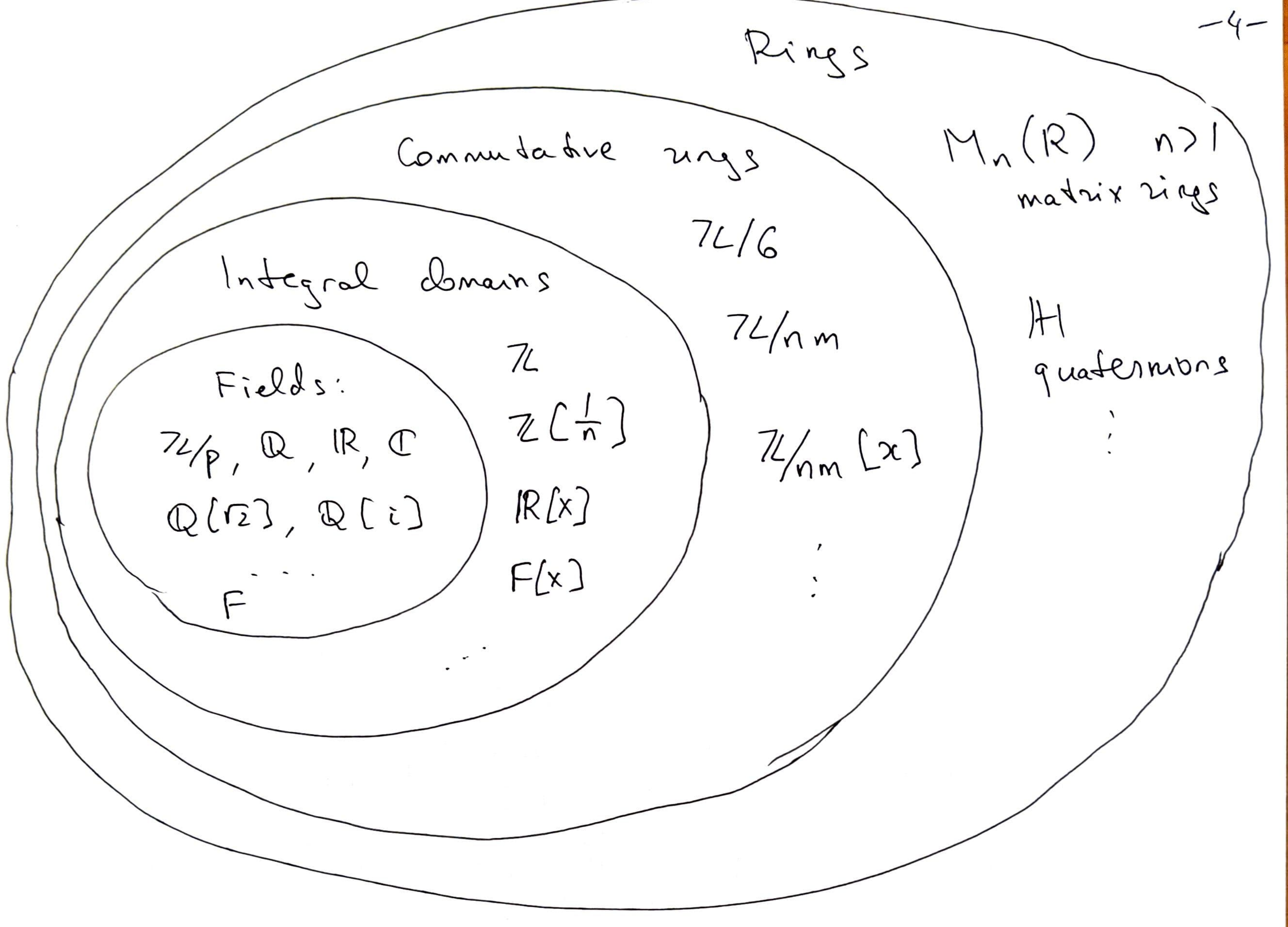
divisors of p: 1 and p.

$\Rightarrow$ for some integers s, t: $\underline{1 = sa + tp}$

$\Rightarrow sa - 1 = -tp \Rightarrow sa \equiv 1 \pmod p \Rightarrow s$ is the inverse of a in $\mathbb{Z}/p$

$[s][a] = [1] \Rightarrow [s] = [a]^{-1}$

$\mathbb{Z}/p$ is an example of a finite field



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

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

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

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

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

lemma holds for F an integral domain, in general

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

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

integral domain   field

$\mathbb{Z} \rightsquigarrow \mathbb{Q}$

$n \rightsquigarrow \frac{1}{n}$ invert all non-zero elements.

Cannot do this if R has zero divisors: $rs = 0$

$r, s \neq 0$

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

:(

Can do this procedure with any integral domain

Integral domain R $\Rightarrow$ Field F

$F = \text{Frac}(F)$

field of fractions

Invert every nonzero element of R.

Need element of the form $\frac{a}{b}$, $b \neq 0$

$\frac{a}{b} = \frac{c}{d}$ iff $ad = bc$.

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

Introduce equivalence relation on this set

$(a, b) \sim (c, d)$ iff $ad = bc$

<u>lemma</u> this is an equivalence relation.

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

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

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

multiply by f mult. by b

$adf = bcf = bde \Rightarrow adf = bde$ $afd = bed \underset{\text{c. law}}{\Rightarrow} af = be$ $\square$

Define Frac(R) as the set of equivalence classes

Next, define addition and multiplication on Frac(R) by

$bd \neq 0$ in R

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}, \quad \left(\frac{a}{b}\right)\left(\frac{c}{d}\right) = \frac{ac}{bd}$$

Need to check they are well-defined

For example, if $\frac{a'}{b'} = \frac{a}{b}$, check that $\frac{a'}{b'} \cdot \frac{c}{d} = \frac{a}{b} \cdot \frac{c}{d}$ $\quad (a'c, b'd) \sim (ac, bd)$

$(a'c, b'd) \overset{?}{\sim} (ac, bd)$

$a'c\,b\,\underset{\smile}{d} \overset{?}{=} acb'\underset{\smile}{d}$ $\quad \overset{\text{use cancellation law}}{\Longleftrightarrow}$ $\quad a'bc \overset{?}{=} ab'c$ $\qquad$ Since $(a',b') \sim (a,b)$

$a'b = b'a$

$\Downarrow$

$a'bc = ab'c$

true

multiply by cd

Exercise: Check that addition is well-defined (does not depend on choices of representatives)

If $\frac{a}{b} = \frac{a'}{b'}$ (or $(a,b) \sim (a',b')$) then $\frac{a'}{b'} + \frac{c}{d} = \frac{a}{b} + \frac{c}{d}$

$ab' = a'b$

$(a'd + b'c, b'd) \sim (ad+bc, bd)$

Exercise with this addition and multiplication, Frac(R) is a field.

a) Check that Frac(R) under addition is an abelian group

Zero element is $\frac{0}{1}$; check that $\frac{0}{1} = \frac{0}{r}$ for any $r \neq 0$

b) check that Frac(R) is associative, commutative under multiplication

Identity is $\frac{1}{1}$; also check that $\frac{1}{1} = \frac{r}{r}$ for any $r \neq 0$.

c) check distributivity

d) Cancellation law: $\frac{ar}{br} = \frac{a}{b}$ if $r \neq 0$.

e) Frac(R) is a field, $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$, if $a \neq 0$ $\leftarrow$ $\frac{a}{b} = \frac{0}{1}$ iff $a = 0$.

Write element $\frac{a}{b}$ as ab^{-1}.

Prop the map $R \xrightarrow{i} \mathrm{Frac}(R)$ is an injective homomorphism of rings. R an integral domain

$i(a) = \frac{a}{1}$. i respects $+, \cdot$, takes 1 to 1 $i(1) = \frac{1}{1} = 1$

$i(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = i(a) + i(b)$ We just write a for $\frac{a}{1}$.

$i(ab) = \frac{ab}{1} = \frac{a}{1} \cdot \frac{b}{1} = i(a)\, i(b)$. write $\frac{a}{b}$ as ab^{-1}

$\frac{a}{b} = \frac{a}{1} \cdot \frac{1}{b} = a \cdot b^{-1}$

Exercise: prove injectivity.

$\frac{b}{1} \cdot \frac{1}{b} = \frac{b}{b} = 1$ in $\mathrm{Frac}(R)$

Example: 1) If R is a field, $\mathrm{Frac}(R) = R$. Every nonzero element is already invertible in R. $\frac{a}{b} \in \mathrm{Frac}(R)$, $b \neq 0$.

$\frac{a}{b} = \frac{(ab^{-1})b}{b} = \frac{ab^{-1}}{1}$ $\frac{a}{b} = i(ab^{-1})$, $ab^{-1} \in R$. Complete the argument.

2) $\mathrm{Frac}(\mathbb{Z}) \simeq \mathbb{Q}$.

Back to homomorphisms:

$\alpha : R \to S$ homomorphism

$\alpha(a+b) = \alpha(a) + \alpha(b)$ respects addition

$\alpha(ab) = \alpha(a)\,\alpha(b)$ respects multiplication

$\alpha(1) = 1$ identity to identity.

as for sets

$\mathrm{Im}(\alpha) = \{ s \in S \mid s = \alpha(a) \text{ some } a \text{ in } R \} = \{ \alpha(a) \mid a \in R \}$

image of α; image of R under α

Prop $\mathrm{Im}(\alpha)$ is a subring of S. Exercise.

$\mathrm{Ker}(\alpha) = \{ a \in R \mid \alpha(a) = 0 \}$ kernel of α; a subset of R.

α is a homomorphism of abelian groups $\Rightarrow \ker(\alpha) \subset R$ is an abelian subgroup under addition.

$\ker(\alpha) = \{a \in R \mid \alpha(a) = 0\}$.

1). If $a \in \ker(\alpha)$, $b \in R \Rightarrow ab \in \ker(\alpha)$.

Need to check $\alpha(ab) = \alpha(a)\alpha(b) = 0 \cdot \alpha(b) = 0$. True

$\Rightarrow \ker(\alpha)$ is closed under multiplication by elements of R.

$\ker(\alpha) \subset R$ is an abelian subgroup of R under the addition operation, and closed under multiplication by elements of R

Example 1) $\mathbb{Z} \xrightarrow{\alpha} \mathbb{Z}/n$ $\quad \alpha(a) = a \pmod{n}$ $\quad \alpha(a) = a + n\mathbb{Z}$

$\ker(\alpha) = n\mathbb{Z} = \{na \mid a \in \mathbb{Z}\}$. $\quad n\mathbb{Z}$ - abelian subgroup, closed under mult.

2) Lemma any homomorphism $\alpha : R \to S$ is injective iff $\ker(\alpha) = \{0\}$

$\{0\}$ is the smallest possible kernel for a homomorphism.

$\ker(\alpha)$ always contains 0, for any homomorphism α

To prove lemma:

If α is injective, $\ker(\alpha)$ contains unique element $0 \in R$.

$$\begin{array}{cccc} \alpha : & R & \longrightarrow & S \\ & \cup & & \cup \\ & \ker(\alpha) & & \operatorname{im}(\alpha) \\ & \text{ideal of } R & & \text{subring} \end{array}$$

If $\ker(\alpha) = \{0\}$ and α not injective $\Rightarrow$

$\exists\, a, b \in R$, $a \neq b$ such that $\alpha(a) = \alpha(b) \Rightarrow$

$\alpha(a) - \alpha(b) = 0$, $\alpha(a-b) = 0$ $\Rightarrow a - b \in \ker\alpha$, $a - b \neq 0$ Contradiction.

Similar to homomorphisms of groups $\quad \alpha : G \to H$ group

α injective $\Leftrightarrow \ker(\alpha) = \{1\}$ trivial subgroup.