Algebra I: Rings: Return exams; discuss curves.
• Mention my talk.

Lecture 13

Def: A ring is a set with binary ops $+, \cdot$ s.t.

1). $(R,+)$ is an abelian gp.

2). $\cdot$ is assoc.

3). $\cdot$ is dist. over $+$:

$(a+b)c = a\cdot c + b\cdot c$ $\quad \forall a,b,c \in R$.

$a\cdot(b+c) = ab+ac$

R is commutative if $\cdot$ is commutative.

R has an identity (has 1) if $\exists\, 1 \in R$,

$1\cdot a = a\cdot 1 = a \quad \forall\, a \in R$.

identity of $+$ is 0. additive inverse of a is $-a$.

— o —

Note: If R has 1 (normally true), then
$(R,+)$ is automatically abelian if distributive:

$a+a+b+b = (1+1)a + (1+1)b = (1+1)(a+b) = (a+b)+(a+b) = a+b+a+b$

$\Rightarrow a+b = b+a$.

So this is not a strong restriction.

Def: R with $1 \neq 0$ is a division ring if

every non-zero elt has a mult inverse.

A commutative division ring is a field.

Ex: Most important example to keep in mind:
$(\mathbb{Z}, +, \cdot)$. Its not a division ring, e.g., 2^{-1} DNE in $\mathbb{Z}$.

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are also rings, and even fields.

Ex: The next example you likely saw was matrices.

e.g. $\mathrm{Mat}_{n\times n}(\mathbb{R})$.
under matrix + and $\cdot$.
Some elts dont have inverses (if $\det \neq 0$).

Ex: Given R an ab. gp. under $+$, define the trivial ring by setting $a \cdot b = 0 \ \forall a, b$.

If $R = \{0\}$, then this is the zero ring $R = 0$.
Not very interesting...

Ex: Quaternions.
Recall: $i^2 = j^2 = k^2 = -1$.

$ij = k$
$ji = -k$.

$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$.
Not commutative with 1.

Ex: $\emptyset \neq X$ a set, A a ring.
the set R of f's $f: X \to A$ under pointwise $+$ and $\cdot$ is a ring.

re. $(f+g)(x) = f(x)+g(x)$ ↑ takes place in A!

Also, $C^k(\mathbb{R})$ is a ring. ← k-times continuously differentiable fcns $\mathbb{R}\to\mathbb{R}$. $k \in \mathbb{N}\cup\{\infty\}$

Important ex: Polynomials / R, R a ring.

$R[x] := \{a_0 + a_1 x + \cdots + a_n x^n \mid a_0,\dots,a_n \in R\}$

as fcns or as formal. (not the same over finite fields)

Power series ring: $R[[x]] = \{a_0 + a_1 x + \cdots + x^n + \cdots \mid a_0,\dots,a_n,\dots \in R\}$

$\cong R^{\mathbb{N}} = \{\text{sequences of elts of } R\}$.

formal, may converge only at $x=0$ (radius 0).

$(a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}} = (a_n+b_n)_{n\in\mathbb{N}}$

$(a_n)\cdot(b_n) = \left(\sum_{k=0} a_k b_{n-k}\right)_{n\in\mathbb{N}}$ ← Cauchy product.

Ex: $\mathbb{Z}/n\mathbb{Z}$!

Ex: Other rings of this.

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

Gaussian integers

Ex: $2\mathbb{Z}$ is a ring w/o 1!

Facts (Exercise): R ring.

1). $0a = a0 = 0$ $\forall a \in R$.

2). $(-a)b = a(-b) = -(ab)$.

3). $(-a)(-b) = ab$.

4). If R has 1, then its unique, $-a = (-1)a$.

works just like $\mathbb{Z}$!

Def: $a \neq 0 \neq a \in R$ is a zero-divisor if:

$\exists$ $b \neq 0$, $ab = 0$ or $ba = 0$.

If R has $1 \neq 0$, u is a unit if

$\exists$ $v \in R$, $uv = vu = 1$.

the set of units $= R^\times$.

Ex 1. In $\mathbb{Z}/6\mathbb{Z}$, 2 is a 0-divisor, as $2 \cdot 3 = 0$.

- In $\mathbb{Z}$, ± 1 are the only units.
- In $\mathbb{Z}[i]$, $\pm 1, \pm i$ are the units.

- A field is a comm. ring R with $1 \neq 0$, s.t. $F^\times = F \setminus \{0\}$.

- 0 zero divisors aren't units:

- e.g.: If $ab = 0$, where $b \neq 0$, and $va = 1$, $v \in R$,

then $b = 1b = (va)b = v(ab) = v0 = 0$ $*$.

$\Rightarrow$ fields don't have 0-divisors

- In $(\mathbb{Z}/n\mathbb{Z})^\times = \{0 \leq m < n-1 \mid (m,n) = 1\}$. (discussed in book)

So $\mathbb{Z}/n\mathbb{Z}$ is a field $\iff$ n is prime.

fields: adjoin algebraic #s (roots of polys.) to $\mathbb{Q}$.

Quadratic fields.

Simplest case: $\mathbb{Q}(\sqrt{D})$, $D \neq \square \cdot \Sigma \mathbb{N}$.
(easiest when $D<0$). (can factor out $\square$s to get $\square$-free D).

Parts we'll work

$\mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D} \mid a, b \in \mathbb{Q}\}$, usual $+, \cdot$ in $\mathbb{C}$.
"degree 2".

Inverses: $(a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2 \neq 0$ as $\sqrt{D} \notin \mathbb{Q}$.

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

ex: $\mathbb{Q}(i)$: $D = -1$.
usual.
$a^2 - Db^2 = a^2 + b^2$. norm in $\mathbb{C}$.

Defn: A comm. ring $\neq 0$ is an integral domain if no zero divisors.

Prop: $a \neq 0$ not a zero divisor, Then
$ab = ac \Rightarrow b = c$ (cancel a's).

Pf: $ab = ac \Rightarrow a(b-c) = 0 \Rightarrow b - c = 0$.
($a \neq 0$) for not a zero-div.

Cor: Finite integral domains are fields:

Pf: R finite integral domain, $0 \neq a \in R$.
map: $R \to R$.
$x \mapsto a \cdot x$
injective by prop.
$|R| = |R| \Rightarrow$ also surjective, s.o. $\exists\, b$, $ab = 1$.

Def^n A subring of R is a subgp closed under ·.

Test: Given a subset of R, check $\neq \emptyset$, closed under $-$, ·.

Ex: nR subring R, $n \in \mathbb{N}$.

Rings of integers in quad. fields: assume $D \neq$ sq free.

$$\omega = \begin{cases} \sqrt{D} & D \equiv 2, 3 \pmod 4 \\ \frac{1+\sqrt{D}}{2} & D \equiv 1 \pmod 4. \end{cases}$$

$\mathcal{O}_D = \mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$ = ring of ints of $\mathbb{Q}(\sqrt{D})$

Works like $\mathbb{Z} \subseteq \mathbb{Q}$.

Norm: $\mathbb{Q}(\sqrt{D}) \to \mathbb{Q}$
$a + b\sqrt{D} \mapsto a^2 - Db^2$.

It's multiplicative; $N(\alpha)N(\beta) = N(\alpha\beta)$ (not hard to check)

Easy to check $N(\alpha) \in \mathbb{Z}$ $\forall \alpha \in \mathcal{O}_D$.

α unit in $\mathcal{O}_D \Rightarrow \alpha\beta = 1$ some β $\Rightarrow N(\alpha)N(\beta) = 1 \Rightarrow N(\alpha) = \pm 1$.
($N(\alpha), N(\beta) \in \mathbb{Z}$)

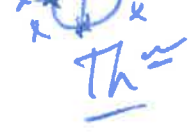
If $N(\alpha) = \pm 1$, then $(a+b\omega)^{-1} = \pm(a + b\bar{\omega}) \in \mathcal{O}_D$
$\alpha = a + b\omega$.

$$\bar{\omega} = \begin{cases} -\sqrt{D} & D \equiv 2,3 \\ \frac{1-\sqrt{D}}{2} & D \equiv 1 \end{cases}$$

So $N(\alpha) = \pm 1 \iff \alpha$ is a unit in $\mathcal{O}_D$ (Check Golden Ratio)

$\mathbb{Z}[i]$ Pell's eq^n: $x^2 - Dy^2 = \pm 1$. (Fibonacci formula)

$D = -1$ solns = fourth roots of unity in $\mathcal{O}_D$



Th^m: $D < 0$: $\mathcal{O}_D^\times = \begin{cases} \{\pm 1, \pm i\} & D = -1. \\ \{\pm 1, \pm\rho, \pm\rho^2\} & D = -3. \\ \{\pm 1\} & \text{else.} \end{cases}$ $\rho = \frac{-1+\sqrt{-3}}{2}$.

$D > 0$: $\exists \varepsilon_D$, $\mathcal{O}_D^\times = \{\pm \varepsilon_D^n, n \in \mathbb{N}\}$. Fundamental unit

$\mathcal{O}_D^\times \cong \mathbb{Z}/2 \times \mathbb{Z}$ rank 1 abelian

Ex: ~~R an int domain~~ $R[x]$, $(R[x])^\times = R^\times$

To Here.

21. $R[x]$ is an integral domain.

Pf 1). $p(x)$ unit $\Rightarrow p(x)q(x) = 1$ (one containment clear.)

$\Rightarrow \deg p + \deg q = 0$

$\Rightarrow \deg p = \deg q = 0$

$\Rightarrow p, q \in R$, and $pq = 1 \Rightarrow p, q \in R^\times$.

2). R int. domain, ~~$pq = 0$~~ ~~$p(x)q(x) = 0$~~ $p, q \neq 0$,

$p = a_0 + \cdots + a_n x^n$

$q = b_0 + \cdots + b_m x^m$

$a_n, b_m \neq 0$

leading term.

$\Rightarrow pq = a_n b_m x^{m+n} + \cdots$

$\neq 0$ as R is an int. domain $\Rightarrow$ ~~$\neq 0$~~

HW announced.

bring exams.

Ex: Group rings:

R comm. ring w/ $1 \neq 0$

$G = \{g_1, \ldots, g_n\}$ a finite gp. (under $\cdot$).

Group ring RG (or G w/ coeffs. in R).

$= \{a_1 g_1 + \cdots + a_n g_n \mid a_1, \ldots, a_n \in R\}$

formal sums

Addition: $(a_1 g_1 + \cdots + a_n g_n) + (b_1 g_1 + \cdots + b_n g_n)$

$= (a_1 + b_1) g_1 + \cdots + (a_n + b_n) g_n$

(component-wise!)

Multiplication: use $(ag_i)(bg_j) = (ab)(g_i g_j) = (ab) g_k$.

extend linearly

Extra time: $e^{\pi i / 3}$