Groups & Rings: Lecture #15

Introduction to rings (§16.1 – 16.2)

- Groups vs rings
- Definition and examples
- Properties of elements and rings
- Subrings
- Underlying group and group of units
- Integral domains and fields
- Characteristic of field/ring

Groups vs rings

Formal similarities

- homomorphism, subgroup, quotient group
- isomorphism theorems, correspondence thm

(many other alg. structures: vector fields, modules
graded rings, graded modules)

rich class

Groups: abelian groups, p-groups, finite groups
Rings: commutative rings ⊃ integral domains ⊃ fields

very rich structure
in contrast to abel. groups

(finite rings not so rich)

Groups: normal subgroups vs **Rings:** ideals

Definition & examples

usually juxtaposition

Def: A ring R is a set w/ 2 operations $+, \cdot$ (or $\oplus, \odot$)

- $(R,+)$ is an abelian group $\left(\begin{array}{l} \exists \text{ unit elt } 0: 0+r=r+0=r \\ \exists \text{ add inv } -r: -r+r=r+-r=0 \\ + \text{ is comm}: r+r'=r'+r \end{array} \quad \forall r, r' \in R\right)$
- Multiplication is ass & dist.

ass: $(rs)t = r(st)$ dist: $r(s+t) = rs+rt$
$(r+s)t = rt+st$

Ex: (1) $\mathbb{Z}$ (integral domain)

(2) $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ (comm w/ id.)

(3) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ (fields)

(4) $M_n(R)$ $(n\times n)$-matrices w/ elts in some ring R (not commutative if $n>1$)

(5) $C([0,1])$, $C^1([0,1])$, $C^\infty([0,1],\mathbb{C})$, $\mathrm{Fun}([0,1],R)$ R rings

cont fcn $[0,1]\to\mathbb{R}$ fcn $[0,1]\to\mathbb{R}$ f' is cont. ∞ differentiable fcns $[0,1]\to\mathbb{C}$

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

(commutative if R is comm)

(6) $R[x] = \{p(x) = \sum_{d=0}^{n} a_d x^d : n\in\mathbb{N}, a_d \in R\}$ R for some comm ring

(the most important example) (commutative)

Non-ex: $GL_n(\mathbb{R})$ group under mult, not closed under add

not a ring.

Prop. 16.8: (i) $0\cdot x = x\cdot 0 = 0$

(ii) $x\cdot(-y) = (-x)\cdot y = -(x\cdot y)$

pf: (i) $x\cdot(0+0) = x\cdot 0 + x\cdot 0 \Rightarrow x\cdot 0 = 0$

(ii) $0 = x\cdot(y+(-y)) = x\cdot y + x\cdot(-y) \Rightarrow x\cdot(-y) = -(x\cdot y)$

Properties of rings & elts

Def: R ring, $r \in R$

(1) r is a mult. identity if $r \cdot s = s = s \cdot r \quad \forall s \in R$ (book: unity)

Easy: if $\exists$ mult id $\Rightarrow$ unique. Denoted 1 or 1_R

(2) r is invertible if $\exists r^{-1}: rr^{-1} = 1 = r^{-1}r$ (common: unit)

(3) r is zero divisor if $\exists s \neq 0: rs = 0$ or $sr = 0$ (book does not allow 0 as a zero divisor)

(4) r is nonzero divisor or regular if not zero divisor.

Ex: $\mathbb{Z}/10\mathbb{Z}$ $\quad 2 \cdot 5 = 0 \quad$ 2, 5 are zero divisors (4, 6, 8)

$2|0, \quad 5|0$

inv. elts $\quad 1, 3, 7, 9 \qquad 1^{-1} = 1, \quad 3^{-1} = 7, \quad 7^{-1} = 3, \quad 9^{-1} = 9$

Def: A ring R is

(a) ring w/ mult identity (ring w/ 1) if $\exists 1_R$ ($1 = 0$ is allowed! but not in book)

(b) commutative if $xy = yx \quad \forall x, y \in R$

(c) integral domain if commutative w/ identity $1 \neq 0$ and 0 is the only zero-divisor

(d) division ring (or skew field) if has identity and every nonzero elt is invertible

(e) field if commutative division ring.

Ex: $\mathbb{H}$ quarternions, $\mathbb{R}\langle 1, i, j, k\rangle \quad ij = k = -ji, \ldots$

$\cong \mathbb{R}^4$ as v.sp.

Ex: $\mathbb{O}$ octonions ($\cong \mathbb{R}^8$ as a v.sp) $\boxed{\text{non-ass div. ring}}$

(1, 2, 4, 8) – theorem

Thm: (Kervaire, Milnor '58) $\mathbb{R}, \mathbb{C}, \mathbb{H}, \mathbb{O}$ are the only real non-ass div algebras.

Subrings

Exc: In the following: $\exists 1_R$?, comm.? int. dom.? fields?

(a) $3\mathbb{Z} = \{\dots, -6, -3, 0, 3, 6, \dots\}$ comm, no 1 (an ideal)

(b) $\mathbb{Z}_{10}$ (comm w/ id, not ID)

(c) $\{a + b\sqrt{2} : a, b \in \mathbb{Q}\} \underset{v.sp}{\cong} \mathbb{Q}^2$ w. basis $1, \sqrt{2}$ $\leftarrow$ ID

(d) $\{a + b\sqrt[3]{2} : a, b \in \mathbb{Q}\}$ (not ring $\sqrt[3]{2} \cdot \sqrt[3]{2} = \sqrt[3]{4} \notin \{a + b\sqrt[3]{2}\}$)

(e) $\{a + bi : a, b \in \mathbb{Q}\}$ $\quad i^2 = -1$ field (Gaussian numbers)

(f) $\{0\}$ comm ring! $(0 = 1)$ not ID/field: by def $0 \neq 1$ in those

the "zero ring"

Multiplication:
$(a+b\sqrt{2})(c+d\sqrt{2})$
$= ac + ad\sqrt{2} + bc\sqrt{2} + 2bd$
$= (ac+2bd) + (ad+bc)\sqrt{2}$

Identity: $1 = 1 + 0\sqrt{2}$

Norm: $N(a+b\sqrt{2})$
$= (a+b\sqrt{2})(a-b\sqrt{2})$
$= a^2 - 2b^2 \in \mathbb{Q}$
$N(rs) = N(r)N(s)$
$N(r) = 0 \Leftrightarrow r = 0$
$\Rightarrow$ integral domain

Rmk: Ex (c) subring of $\mathbb{R}$. $\Rightarrow$ int. domain
Ex (e) — " — $\mathbb{C}$. $\Rightarrow$ — " —

Def: A subset $S \subset R$ is a subring if S w/ same $+, \cdot$ is a ring.
That is, $x, y \in S \Rightarrow x + y, -x, xy \in S$. and $0 \in S$
(S is closed under addition, add. inverses, mult.)

Exc: R is an integral domain $\Rightarrow$ S is an integral domain
R is commutative $\Rightarrow$ S is commutative

Ex: $3\mathbb{Z} \subset \mathbb{Z}$ is a subring but usually one requires:
if $1_R \in R \Rightarrow 1_R \in S$. (but the book does not)

Sometimes: Ring = ring w/ identity
Rng = ring w/o — " — "rungs"

Two groups associated to a ring

Def: R ring. The underlying group is $(R,+)$, an abelian group.

Def: R ring w/ identity. The group of units is
$R^\times = \{r \in R : r \text{ invertible}\} \subset R$.
(= unit)
A group under mult. (abelian if R commutative)
$1 \in R^\times$, $r \in R^\times \Rightarrow r^{-1} \in R^\times$

Ex: $(\mathbb{Z}_{10})^\times = \{1,3,7,9\}$ abelian group.
Exc: Which abelian group is this? $(\mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_4)$?
Ex: $M_n(\mathbb{Q})^\times = GL_n(\mathbb{Q})$

Exc: $M_2(\mathbb{Z})^\times = ?$ $\quad \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix} \notin M_2(\mathbb{Z})$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \in M_2(\mathbb{Z}) \text{ if } \det \in \{\pm 1\}$$

$\det(A) \in \mathbb{Z} \quad A \in M_2(\mathbb{Z})$

$$1 = \det(AA^{-1}) = \underset{\mathbb{Z}}{\underset{\cap}{\det(A)}}\,\underset{\mathbb{Z}}{\underset{\cap}{\det(A^{-1})}} \Rightarrow \det(A) \in \mathbb{Z}^\times$$

$\det(A) = \pm 1$

In general:
$$M_n(\mathbb{Z})^\times = \{A \in M_n(\mathbb{Z}) : \det(A) \in \{\pm 1\}\}$$
$$M_n(R)^\times = \{A \in M_n(R) : \det(A) \in R^\times\} \quad R \text{ comm ring}$$

Integral domains

Recall: $xy = 0 \overset{\text{ID}}{\Longrightarrow} x = 0$ or $y = 0$

Gaussian integers

Ex: $\mathbb{Z}[i] = \{x + yi : x, y \in \mathbb{Z}\} \subset \mathbb{Q}[i] \subset \mathbb{C}$

subring of a field $\Rightarrow$ integral domain.

Exc: R int. domain $\Rightarrow$ $R[x]$ int. domain

Prop 16.15: R int. domain $\Leftrightarrow$ cancellation holds in R

$(xy = xz,\ x \neq 0 \Rightarrow y = z)$

pf: $xy = xz \Leftrightarrow xy - xz = 0 \Leftrightarrow x(y-z) = 0$

$\Rightarrow x = 0$ or $y = z$

if R int. domain

$xy = 0 \Leftrightarrow xy = x \cdot 0 \Leftrightarrow x = 0$ or $y = 0$

if cancellation holds

$\square$

Thm 16.16: (exam 2019-08-12, prb 4b)

A finite integral domain R is a field.

pf: Pick $r \neq 0$ in R. Consider $\{1, r, r^2, r^3, \dots\}$ finite set

$\Rightarrow \exists m < n$ pos integers $r^m = r^n \underset{\text{canc.}}{\Longrightarrow} r^{n-m} = 1 \Leftrightarrow r^{-1} = r^{n-m-1}$. $\square$

Rmk: $r \in R$ is nonzero divisor $\Leftrightarrow$ $m_R : R \longrightarrow R$, $s \longmapsto rs$ injective (grp hom under $+$)

R commutative

Characteristic

Integral domains can be divided into 2 classes: characteristic zero & finite characteristic ("char. p").
The latter is divided into one class for each prime p.

char 0

Ex: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}$, $\mathbb{R}[x]$

$n := 1+1+1+1+\cdots+1 \neq 0$

$nx = x+x+x+x+\cdots+x \neq 0$

char p

Ex: $\mathbb{Z}_p$, $\mathbb{Z}_p[x]$, $M_n(\mathbb{Z}_p)$

$p := 1+1+1+\cdots+1 = 0$

$px = x+x+x+\cdots+x = 0$

Def: Let R be an integral domain. The characteristic of R is the smallest positive integer n s.th. $nr = \underbrace{r+r+\cdots+r}_{n \text{ terms}} = 0 \ \forall r$ or $n=0$ if no such positive n exists.

Lem 16.18: $\operatorname{char} R = \begin{cases} |1| & \text{if finite} \\ 0 & \text{o/w} \end{cases}$ $|1|$ = order of 1 in the group $(R,+)$

"pf": $r+r+\cdots+r = 1\cdot r + 1\cdot r + \cdots + 1\cdot r$
$= n\cdot r$

Thm 16.19: R int. domain $\Rightarrow$ char(R) prime or 0.

Ex: $\mathbb{Z}_p$ int. dom w/ char $= p$.

Ex: $\mathbb{Z}_{10}$ not int. dom.