Algebra6 25032019

Direct product: $(G_1,*_1), (G_2,*_2)$

$G = G_1 \oplus G_2 \quad * = (*_1,*_2)$

Example $G_1 = \mathbb{Z}_4 \quad G_2 = U(12)$

$G_1 \oplus G_2 = \{(a,b) \mid a \in G_1, b \in G_2\}$.

$G = \{(a,b) \mid a \in \mathbb{Z}_4, b \in U(12)\}$.

$* = (*_1,*_2)$: $(a,b), (c,d) \in G$

$(a,b) * (c,d) = (a *_1 c, b *_2 d)$

$(a,b), (c,d) \in \mathbb{Z}_4 \oplus U_{12}$:

$(a,b) * (c,d) = (a+c \bmod 4, b \cdot d \bmod 12)$.

$G_1 \oplus G_2$ forms a group: $e = (e_1, e_2)$

$(a,b)^{-1} = (a^{-1}, b^{-1})$

Likewise $(G_1,*_1) \oplus (G_2,*_2) \oplus \cdots \oplus (G_4,*_4)$

$|\mathbb{Z}_4 \oplus U_{12}| = 4 \cdot 4 = 16$

$|G| = |G_1| \cdot |G_2|$

$\mathbb{Z}_2 \oplus \mathbb{Z}_3 \quad |(1,0)| = 2 \quad |(0,1)| = 3$

$|(1,1)| = 6 \qquad |\mathbb{Z}_2 \oplus \mathbb{Z}_3| = 6$

$\Rightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_3$ is cyclic

$\Rightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_6$

$(1,1) \mapsto 1$ (generator to generator)

$(0,2) \mapsto 2$

$(1,0) \mapsto 3$

$(0,1) \mapsto 4$

$(1,2) \mapsto 5$

$(0,0) \mapsto 0$

Theorem Let $|G| = 4$ then

either $G \cong \mathbb{Z}_4$

or $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ ← Klein group

Proof Suppose $a \in G \Rightarrow |a| \leq 3$

$a \neq e \Rightarrow |a| = 2$

$G = \{e, a, b, a+b\}$ $e \mapsto (0,0)$

$a \mapsto (1,0)$

$b \mapsto (0,1)$

$a+b \mapsto (1,1)$

$(a,b) \in G \oplus G$

$|a|=n_1$, $|b|=n_2$ $\Rightarrow$ $|(a,b)| = lcm(n_1,n_2)$

Thm. $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \cong \mathbb{Z}_{n_1 n_2} \iff lcm(n_1,n_2) = n_1 n_2$
$\iff gcd(n_1,n_2)=1$

Example $\mathbb{Z}_3 \oplus \mathbb{Z}_4 \cong \mathbb{Z}_{12}$
$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \not\cong \mathbb{Z}_4$
$\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k} \cong \mathbb{Z}_{n_1 n_2 \cdots n_k} \iff gcd(n_i,n_j)=1$ $i \neq j$

Application
Let $n_1, \dots, n_k$ be such that $gcd(n_i,n_j)=1$ $i \neq j$

$\forall k_1, \dots, k_l$
$\exists k$ $k \bmod n_1 = k_1 \bmod n_1$
$k \bmod n_2 = k_2 \bmod n_2$
$\vdots$
$k \bmod n_l = k_l \bmod n_l$

Chinese Remainder Theorem

Thm. Let G be a commutative group, $|G|<\infty$
then $G \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k}$

Example $\mathbb{Z}$ $3+4$ $3 \cdot 4$
$(\mathbb{Z},+,\cdot)$ is a ring:
- a group w.r.t. $+$, commutative
- $\forall a,b,c \in \mathbb{Z}$: $a.(b+c) = a.b + a.c$ (distributive)
distributive
- $a.(b.c) = (a.b).c$ associative

$(R,+,\cdot)$, can be $1 \in R$ that has the property: $1.a = a.1 = a$.

Example $(\mathbb{Z},+,\cdot)$; $(2\mathbb{Z},+,\cdot)$
1 ; $\nexists$ 1

A ring is $(R,+,\cdot)$
R: a set
$(R,+)$ is a commutative group
$\forall a,b,c \in R$: $a.(b+c) = a.b + a.c$ $\{(b+c).a = b.a + c.a$

R can have $1 \in R$ $\forall a \in R$: $1 \cdot a = a \cdot 1 = a$
require $0 \neq 1$.

If $1 \in R$:

- $0 \cdot a = 0$
- $(-1) \cdot a = -a$

$0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a$

$0 \cdot a + (-(0 \cdot a)) = 0 \cdot a + 0 \cdot a + (-(0 \cdot a))$

$0 = 0 \cdot a + 0$

$= 0 \cdot a$

- $(-1) \cdot a + a = (-1) \cdot a + 1 \cdot a$
$= (-1+1) \cdot a$
$= 0 \cdot a = 0$
$\Rightarrow (-1) a = -a$

- Subring $(S,+,\cdot)$ is a subring of $(R,+,\cdot)$ if $S \subseteq R$ and S a ring
- Example $2\mathbb{Z}$ is a subring of $\mathbb{Z}$
- Examples of rings: $(\mathbb{Z}_n,+,\cdot)$ $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ $(\mathbb{Q},+,\cdot)$

Example. $R = \mathbb{Z}_6$: $2 \cdot 3 = 0$
$\neq 0$ $\neq 0$
we say 2 and 3 are zero-divisors

- $\mathbb{Z}_7$: find zero-divisors: none
- $\mathbb{Z}_{10}$: " " " : 2,5

Def An integral domain is a commutative ring R, with $1 \in R$ and no zero-divisors.

Examples $\mathbb{Z}_3, \mathbb{Z}_7, \mathbb{Z}_{17}$ are integral domains, $\mathbb{Z}_1, \mathbb{Z}_{10}, \mathbb{Z}_{p \cdot q}$ $p,q>1$
zero divisors

Def. If R is a ring, $1 \in R$ if R is int. dom. then $\text{char}(R) = \min\{n \mid \underbrace{1+1+\dots+1}_{n} = 0\}$.

$= 0$ ✓ $= \emptyset$ ✗

$char(\mathbb{Z}) = 0$

$char(\mathbb{Z}_7) = 7$

Theorem. R is int. dom. then

$char(R) = p$ (p prime) or $char(R) = 0$

proof Assume that $char(R) = p \cdot q$

$p, q > 1$

then $\underbrace{(1+1+\dots+1)}_{p}\underbrace{(1+1+\dots+1)}_{q}$

$= \underbrace{(1+1+\dots+1)}_{pq \text{ x}} = 0$

$\Rightarrow \underbrace{(1+1+\dots+1)}_{p^{\text{th}}} = 0$ or $\underbrace{(1+\dots+1)}_{q} = 0$ ✗

$\Rightarrow$ $char(R) \neq$ prime

Corollary $\mathbb{Z}_n$ is int. dom. $\Leftrightarrow$ n is prime

Thm. If R is an int. dom. and $|R| < \infty$

then R is a field.

Def. Let R be an int. domain, then

R is a field if $(R \setminus \{0\}, \cdot)$ is a group

Examples of field: $(\mathbb{R}, +, \cdot)$; $(\mathbb{Q}, +, \cdot)$

$(\mathbb{Z}, +, \cdot)$ is not a field

proof of theorem: take $a \in R$, $a \neq 0$

$a, a^2, a^3, a^4, \dots a^k, a^{k+1}$

$\Rightarrow i < j$ s.t. $a^i = a^j$

$\Rightarrow a^{i-j} \cdot a^j = a^j$

$a^{i-j} = 1$

$\Rightarrow a \cdot a^{i-j-1} = 1$

$\Downarrow$

$a^{i-j-1} = a^{-1}$

Corollary: $R = \{a+bi \mid a, b \in \mathbb{Z}_3\}$. $|R| = 9$

$i^2 = 2$

R is an integral domain (check) $\Rightarrow$

R is a field