Alg – 24

Ex
Let G be a group of order $56 = 2^3 \cdot 7$
There are at least one 2-Sylow subgroup of order 8 and at least one 7-Sylow subgp of order 7.

$n_2 = 1+2k \mid 2^3 \cdot 7$, $k = 0, 3$

$n_7 = 1+7k \mid 2^3 \cdot 7$, $k = 0, 1$

So there are 1 or 7 2-Sylow subgps of order 8
and there are 1 or 8 7 Syl. ~.
of orders 7

1 — 2-Sylow — order 8
8 — 7 Sylow — " 7

Every non identity element of 7-Sylow subgroup has $|a| \mid |G| = 7$. If there were 8 7-Sylow subgroups of order 7, then there will be 55 elements of order 7.
& at least one 2-Sylow subgroup of order 8

& at most
subgroup of size

So 1 - 2 Syl/w
& 7 - 7 Syl/w

7 - 2 Syl/w
1 - 7 Syl/w

|a| | 8

Only 1 - 2 Syl/w subgroup
of order 8
and only one 7 - Syl/w subgroup
of order 7.

Both are normal

Ex Prove that a group of order
143 is not simple & has
a nontrivial normal subgroup

$N \triangleleft G$ nontrivial means
$N \neq \{e\}$ $N \neq G$:
$\{e\} \subsetneq N \subsetneq G$

Sol $|G| = 143 = 11 \cdot 13$
So G has at least one
11 - Syl/w subgroup of order 11
at least one 13 - Syl/w ... 13

and at least one 13-Sylow -

$n_{11} = 1+11k \mid 11.13$, $k=0$

$\Rightarrow$ only one 11-Sylow subgroup of order 11.

H is normal

$H = xHx^{-1}$ is 11-Sylow subgp $\forall x$

$n_{13} = 1+13k \mid 11.13$, $k=0$

Only one 13-Sylow subgroup K of order 13

$|H \cap K| = 1$

check that $H = \langle x \rangle$?
$K = \langle y \rangle$.

$xy = y^n x$

$\Rightarrow G = H \times K$ cyclic

$H \simeq \mathbb{Z}_{11}$

$\square$

$H \simeq \mathbb{Z}_{11}$

$K \simeq \mathbb{Z}_{13}$

$HK \simeq \mathbb{Z}_{11} \times \mathbb{Z}_{13} \overset{?}{\simeq} \mathbb{Z}_{143}$

Rings, Integral domains (entire ring) fields

A group has one binary operation.
Now we consider alg systems with more than one binary operations.

① $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Z}, +)$ is abelian group $a, b \in \mathbb{Z}$, $\cdot(a,b) = ab$

$\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, satisfying

R_1 $a(bc) = (ab)c$ — associative law

R_2 $a(b+c) = ab + ac$ — left dist

$(b+c)a = ba + ca$ — right dist

$ab = ba$ — commutative

$1a = a \quad \forall\, a \in \mathbb{Z}$.

1 is the multiplicative identity.

$(\mathbb{Z}, +, \cdot)$ is a a commutative ring with identity 1.

Ex. $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$

Ex $n \geq 1$ integer. $K = \mathbb{Q}, \mathbb{R}, \text{or } \mathbb{C}$

$(M_{n\times n}(K), +, \cdot)$, $(M_{n\times n}(K), +)$ is commutative group

$A, B \in M_{n\times n}(K)$,

$$(AB)_{ij} \overset{\text{def}}{=} \sum_{k=1}^{n} (A)_{ik}(B)_{kj}$$

AB is the product

$$(AB)C = A(BC)$$

$$A(B+C) = AB + AC \quad \text{– left}$$

$$(B+C)A = BA + CA \quad \text{– Right}$$

$$(I_n)_{ij} = \delta_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

$$\Rightarrow I_n A = A I_n = A$$

$(M_{n\times n}(K), +, \cdot)$ is a noncommutative ring.

(3) $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}$

$(a+ib) + (c+id) \overset{\text{def}}{=} (a+c) + i(b+d)$ – sum

$(a+ib)(c+id) \overset{\text{def}}{=} (ac-bd) + i(ad+bc)$ prod.

$(a+ib)+(c+id) \overset{\text{def}}{=} (a+c)+i(b+d)$ sum.

$(a+ib)(c+id) \overset{\text{def}}{=} (ac-bd)+i(ad+bc)$ prod.

$(\mathbb{Z}[i], +, \cdot)$ we have

$(\mathbb{Z}[i], +)$ is an abelian group

& $\cdot$ is associative, distr. & commutative with identity $1 = 1+i0$.

$(\mathbb{Z}[i], +, \cdot)$ is a commutative ring with identity is unit.

Def A ring is an ordered triple $(R, +, \cdot)$ where $(R, +)$ is an abelian group and $\cdot : R \times R \to R$ satisfies $\cdot(a,b) = ab \in R$ & satisfies

— $(ab)c = a(bc)$ - asso. law

— $a(b+c) = ab + ac$ - left dist

— $(b+c)a = ba + ca$ - right ...

We write R is a ring when there is no confusion.

$(R, +, \cdot)$ is a commutative ring if $ab = ba \quad \forall a, b \in R$.

iff $ab=ba$

$(R,+,\cdot)$ has a unit or identity iff $\exists\, 1\in R$ s.t. $a1=1a=a$ $\forall a\in R$.

If R has a unit we assume $1\neq 0$

— $R=\{0\}$ to be a ring.

— $R=2\mathbb{Z}=\{2n : n\in\mathbb{Z}.\}$

$(R,+,\cdot)$ is a commutative ring. No identity.

Ex $\left(\mathbb{Z}/n\mathbb{Z}, \oplus_n, \otimes_n\right)$ is a commutative ring with unit. A ring with identity or unit is called a unital ring

ALL OUR RING ARE ASSOCIATIVE RINGS.

Ex $(\mathbb{R}^3,+,\times)$ whose

Abelian group

Ex (non-associative algebras)

$(\mathbb{R}^3, +)$ is abelian group

$\vec{a}, \vec{b} \in \mathbb{R}^3$, $\vec{a} \times \vec{b} \in \mathbb{R}^3$

$$= \det \begin{pmatrix} \vec{i} & \vec{j} & \vec{k} \\ a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{pmatrix}$$

$\vec{a} \times \vec{a} = \vec{0}$

$\vec{a} \times \vec{b} \neq \vec{b} \times \vec{a}$

$\vec{a} \times (\vec{b} + \vec{c}) = \vec{a} \times \vec{b} + \vec{a} \times \vec{c}$

$(\vec{b} + \vec{c}) \times \vec{a} = \vec{b} \times \vec{a} + \vec{c} \times \vec{a}$

But $\vec{a} \times (\vec{b} \times \vec{c}) \neq (\vec{a} \times \vec{b}) \times \vec{c}$

$\vec{i} \times (\vec{i} \times \vec{j}) = \vec{i} \times \vec{k} = -\vec{j}$

$(\vec{i} \times \vec{i}) \times \vec{j} = \vec{0} \times \vec{j} = 0$

$\vec{a} \times (\vec{b} \times \vec{c}) = \vec{b}(\vec{a} \cdot \vec{c}) - \vec{c}(\vec{a} \cdot \vec{b})$

(BAC − CAB rule)

$\vec{a} \times (\vec{b} \times \vec{c}) = (\vec{a} \times \vec{b}) \times \vec{c} + \vec{b} \times (\vec{c} \times \vec{a})$

The set of observables in Q.M is a nonassociative ring (called Jordan ring)

Pasqual Jordan

Jordan

Pasquale Camille Jordan

G/H

Wilhelm Jordan

Gauss-Jordan elimination process

Ex $n \in \mathbb{N}$

$(\mathbb{Z}/n\mathbb{Z}, \oplus_n, \otimes_n)$

$(\mathbb{Z}/n\mathbb{Z}, \oplus_n)$ is a group

and $[a]_n \otimes [b]_n = [b]_n \otimes_n [a]$

dist & has identity $[1]_n$

$\mathbb{Z}/12\mathbb{Z} = \{0,1,2,3,4,5,6,7,8,9,10,11\}$

$(\mathbb{Z}/12\mathbb{Z}, +)$ is a group

$(\mathbb{Z}/12\mathbb{Z}, +, \cdot)$ is a commutative unital ring

David Hilbert coined the term algebraic

David Hilbert coined the term ring (like ring of algebraic integers)

Def. A subset S of R is a subring of a ring R iff $(S, +, \cdot)$ is a ring.

Thm $S \subseteq R$ is a subring $\iff$ (1) $a, b \in S \Rightarrow a - b \in S$

(2) $a, b \in S \Rightarrow ab \in S$

Defn Let R be a unital ring

$$U(R) = \{ a \in R : \exists b \in R \text{ s.t. } ab = 1 = ba \}$$

where 1 is the identity of R

Prop $(U(R), \cdot)$ is a group

Proof. $a, b \in G(R)$

$\exists\, c, d \in R$ s.t. $ac = ca = 1$

& $bd = db = 1$.

$(ab)(dc) = a(bd)c = a(1)c$

$= ac$

$= 1$.

$= 1$.

R

$(dc)(ab) = d(ca)b = d(1)b = db$, $=1$

$ab \in U(R)$

assso. $a \in U(R)$

$a^{-1} \in U(R)$

s.t. $a^{-1}a = aa^{-1} = 1$.

Note $a \in U(R)$ $\exists\, b \in R$ s.t.

$ab = ba = 1$. b is unique(?)

$b = a^{-1}$, called the inverse of 1

If $ca = ac = 1$, then $b = c$

Pf:

Let $(R, +, \cdot)$ be a ring.

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

(2) $(-b)a = -(ba) = b(-a)$ $\forall\, a, b \in R$

(3) $a(b-c) = ab - ac$ $\forall\, a, b, c \in R$

(4) $(-b)(-a) = ab$

If R is unit 1, then

(5) $(-1)a = -a$

(6) $(-1)(-1) = 1$

(6) $(-1)(-1) = 1$

Proof (1) $0 = 0+0$

$a \cdot 0 = a(0+0) = a0 + a \cdot 0$

$\Rightarrow a0 + 0 = a0 = a0 + a0$

By uniqueness of additive identity we get

$a \cdot 0 = 0$.

(2) $0 = 0a = (b + (-b))a$

$= ba + (-b)a$

$(-b)a = -(ba)$. by uniqueness of additive inverse.

Ex $(R_i, +_i, \cdot_i)_{i=1 \ldots n}$ case

rings

$R = R_1 \times R_2 \times \cdots \times R_n$

$a, b \in R$, $a = (a_1 \ldots a_n)$

$b = (b_1 \ldots b_n)$

$a + b = def = (a_1 + b_1, \ldots a_n + b_n)$

& $a \cdot b = (a_1 \cdot b_1, \ldots a_n \cdot b_n)$

then $(R, +, \cdot)$ is a ring.

$R = \mathbb{Z}/2\mathbb{Z} \times M_{2\times 2}(\mathbb{Z})$ is a ring

not commutative

$1_R = (1, I_2)$ is the unit

$\mathbb{Z}[i]$ — Gaussian Integers

Ex 1. $U(\mathbb{Z}) = \{1, -1\}$

2. $U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$

3. $U(M_{n\times n}(\mathbb{R})) = GL(n, \mathbb{R})$

4. $U(M_{n\times n}(K)) = GL(n, K)$

5. $\mathbb{Z}[x]$ = the set of all polynomials

$a_0 + a_1 x + \cdots + a_m x^m$

where $a_0, \ldots, a_m \in \mathbb{Z}$.

$f(x) = a_0 + a_1 x + \cdots + a_m x^m$

$g(x) = b_0 + b_1 x + \cdots + b_n x^n$

$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + c_d x^d$, $d = \max\{m, n\}$

$c_d = a_m + b_n$

$g(x) \cdot g(x)$

v

$$(2+3x+4x^2)+x^2+x^5$$

$$=2+4x+4x^2+x^5$$

$$(2+3x+4x^2)(x+x^5)$$

$$=2x+3x^2+4x^3+5x^2+3x^2+4x^7$$

$$=2x+11x^2+4x^3+4x^7$$

$(\mathbb{Z}[x],+,\cdot)$ is a commutative unital ring. $f(x)=1$ is the unit. poly

$$f(x)=a_0+\dots+a_nx^n \qquad a_n\neq 0$$

$\deg f = n$.

— $\deg(f+g)\le \max\{\deg f(x), \deg g(x)\}$

— $\deg(fg)=\deg f+\deg g(x)$

$$U(\mathbb{Z}[x])=\{1,-1\}$$

$$U(\mathbb{Q}[x])=\mathbb{Q}^*\equiv\mathbb{Q}-\{0\}$$

$$U(\mathbb{R}[x])=\mathbb{R}^*$$

$$U(\mathbb{C}[x])=\mathbb{C}^*$$

U(L[x]) - 4

Note A subring S of a unital ring R need not have the unit.

Ex $S = \{0, 3, 6, 9\} \subseteq \mathbb{Z}/12\mathbb{Z}$

$= \{0, 1, 2, 3, 4, \ldots 11\}$

ring with 1.

$1_S = 9$

$3 \cdot 9 = 3$

$6 \cdot 9 = 6$

$9 \cdot 9 = 9$

Def. R is a ring

$Z(R) = \{x \in R : xa = ax \ \forall a \in R\}$

is called the centre of the ring R

Prop. $Z(R)$ is a subring of R

Def. Let R be a commutative ring with unit 1.

R is called an integral domain or an (entire ring in French) iff $ab = 0 \Rightarrow a = 0$ or $b = 0$

That is R has no zero divisors

a ring

that is . . .

Def. F is a commutative ring with 1. F is a field iff $(F^*, \cdot)$ is a commutative group.