Alg-25

$|G| = 56 = 2^3 \cdot 7$

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

there are either 1 or 7 2-Sylow subgroups of order 8

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

there are one 7-Sylow subgroup of order 7 or 8 7-Sylow ... of order 7

1 — 2-Sylow & one 7-Sylow not possible ?

If p-Sylow then say $p^n \mid |G|$ and $p^{n+1} \nmid |G|$ Then G has ... of order p^n

and $p^{\cdots} \mid 41^{\cdots}$ a p-Sylow subgroup of order $p^{\cdots}$

2-Sylow of $\cdot 8$

7 Sylow $\cdots 7$

If there are 8 7-Sylow subgroups of order 7 each non identity element of 7-Sylow subgroup lies prod 7. There $\underline{48}$ of them

---

Polynomials $F[x]$ and integers $\mathbb{Z}$

Ring $(R, +, \cdot)$ R may be commutative or may have identity 1.

. Let R be a ring. Let $a, b \in R$

Find (1) $(a+b)(a-b)$

(2) $(a+b)^2$

(2) $(a+b)$

Here $x \in R$ $x^2 = x \cdot x$, $n \in \mathbb{N}$

$x^{n+1} = x^n x$ So the powers are inductively defined

$x^n \cdot x^m = x^{n+m}$ $\forall\, n, m \in \mathbb{N}$

$(x^n)^m = x^{nm} = x^{mn} = (x^m)^n$

x^{-2}, may not be. Yes if x is invertible.

$$\left.\begin{aligned}(a+b)(a-b) &= a^2 - ab + ba - b^2 \\ (a+b)(a+b) &= a^2 + ab + ba + b^2\end{aligned}\right\}$$

If $ab = ba$, then $(a+b)(a-b) = a^2 - b^2$

& $(a+b)^2 = a^2 + 2ab + b^2$

Def (1) R is a commutative ring.

$a \in R - \{0\}$ is a zero divisor if

there $b \in R - \{0\}$ s.t. $ab = 0$

there $b \in R - \{0\}$ s.t. $ab = 0$

(2) R is a commutative ring with 1. Then R is an integral domain or integral ring (entire ring) if R has no zero divisors.

3. R is a field iff $(R, +, \cdot)$ is a commutative ring with 1 and $(R^*, \cdot)$ is a group

Note F is a field $\Rightarrow$ It is an integral domain

$ab = 0$. If $a \neq 0 \Rightarrow \bar{a}^{-1}(ab) = \bar{a}^{-1}0 = 0$

$\Rightarrow b = 0$

(4) Let $(R, +, \cdot)$ be a ring with 1

R is a division ring or skew-field iff $(R^*, \cdot)$ is a group

A commutative skew-field is a field

Ex. Let $R = \mathbb{Z}/12\mathbb{Z} = \{[0], \ldots [11]\}$

$[2][6] = 0$, $[3][4] = 0$

So $[2]$ & $[3]$ are zero divisors in $\mathbb{Z}/12\mathbb{Z}$

2. $\mathbb{Z}$ is an integral domain
3. $\mathbb{Q}$, $\mathbb{R}$ & $\mathbb{C}$ are integral domains
4. $\mathbb{Q}$, $\mathbb{R}$ & $\mathbb{C}$ are fields

Thm (1) A finite integral domain R is a field

(2) $\mathbb{Z}/p\mathbb{Z}$ is an integral domain $\iff$ p is prime

(3) p, prime, $\mathbb{Z}/p\mathbb{Z}$ is a finite integral domain. So $\mathbb{Z}/p\mathbb{Z}$ is

integral domain
a field.

Proof (1) Let $\{a_1, \ldots a_n\} = R$ be the fgp

$R \ni a \neq 0$. $f_a : R \to R$ by

$$f_a(x) = ax.$$

$$f_a(x+y) = a(x+y) = ax + ay$$
$$= f_a(x) + f_a(y)$$

$\ker f_a = \{0\}$ as $ax = 0$

$a \neq 0 \Rightarrow x = 0$?

So f_a is injective. R is

finite $\Longrightarrow$ $f_a(R) = R$.

$1 \in R \Rightarrow \exists\, b \in R$

s.t. $f_a(b) = 1$

i.e. $ab = 1 = ba$.

Cf. $ab = 1 = ba$.

FACT. S is finite set

$f : S \to S$ is injective

$\iff$ f is surjective

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

$[a] \neq [0]$ in $\mathbb{Z}/p\mathbb{Z}$

a is not divisible by p

$(a, p) = 1$

$ra + sp = 1$.

$[a][r] + [s]\underbrace{[p]}_{0} = [1]$

$[a][r] = 1$

$[a]^{-1}$ exists &

$[a]^{-1} = [r]$.

$[4][4] = [1]$

In $\mathbb{Z}_5$, $[4][4] = [1]$

$[3][2] = [1]$

Eg

$$\mathbb{Z}[x] = \{ f(x) = a_0 + a_1 x + \cdots + a_n x^n : a_0, \ldots a_n \in \mathbb{Z} \}$$

$f(x) + g(x)$, $g(x) = b_0 + b_1 x + \cdots + b_m x^m$

$$= (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n$$

for $n = m$

$n < m$

$$= \cdots (a_n + b_n)x^n + b_{n+1}x^{n+1} + \cdots + b_m x^m$$

$$f(x)\,g(x) = c_0 + c_1 x + \cdots + c_{m+n} x^{m+n}$$

where $c_k = \sum_{i+j=k} a_i b_j$

$$= \sum_{i=0}^{k} a_i b_{k-i}$$

$(\mathbb{Z}[x], +, \cdot)$ is a commutative ring. In fact it is an integral domain

an integral domain

Ex $\mathbb{Q}[\sqrt{2}] = \{ a+\sqrt{2}b : a,b \in \mathbb{Q} \}$ (rationals)

$(a+\sqrt{2}b)+(c+\sqrt{2}d)$

$= (a+c)+(b+d)\sqrt{2}$ — sum

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

product

$(\mathbb{Q}[\sqrt{2}], +, \cdot)$ is a commutative ring with $1 = 0+\sqrt{2}\cdot 0$. In fact it is an integral domain.

We know more: $\mathbb{Q}[\sqrt{2}]$ is a field

$\mathbb{Z}[\sqrt{-5}]$ is not a UFD

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

Let R be a ring with 1.

Let R be a ring with 1.

Def(1) $\phi \neq J \subseteq R$ is a left ideal of R

iff (i) $a, b \in J \Rightarrow a+b \in J$

(ii) $ra \in J \quad \forall r \in R, \forall a \in J$

(2) J