1/29

$a \equiv b \mod n$ $\quad n \mid a-b \quad \exists k \in \mathbb{Z} \quad nk = a-b$

$A = \mathbb{Z}/n\mathbb{Z}$ $\quad \oplus : A \times A$

$\oplus(([a],[b])) \qquad [a] \oplus [b] = [a+b]$

$$\begin{aligned}[a] &= [x] \\ [b] &= [y]\end{aligned} \Rightarrow \begin{aligned}[a+b] &= [x+y] \\ [ab] &= [xy]\end{aligned}$$

$ab - xy = ab - ax + ax - xy$

(or check notes)

$\mathbb{Z}/n\mathbb{Z} = \{[0],[1],\ldots,[n-1]\}$ (form a partition)

partition on A

$P = \{A_i\}$ $\quad i \neq j \quad A_i \cap A_j = \emptyset$ $\quad$ Ex. $\{a,b,c,d,e,f\}$

$\bigcup A_i = A.$ $\qquad \{\{a\},\{b,c\},\{d,f,e\}\}$

Ex $\mathbb{Z}/18\mathbb{Z}.$ $\qquad [5]\cdot[7]$ $\qquad 18\overline{)35}^{\,1}$

$= [17] = [35]$

$= [-1]$

Comm. ring w/ 1 s.t.

if $ab=0$, then $a=0$ or $b=0$

Def 12 A **ring** R is a set w/ 2 operations $\cdot, +$ (associative)

satisfying the following

i) $(R,+,0)$ is an abelian group.

ii) $\forall a,b,c \in R$ $\quad a\cdot(b+c) = a\cdot b + a\cdot c$ $\quad$ i.e. mult. dist over $+$

$(b+c)\cdot a = b\cdot a + c\cdot a$.

Ex. $(\mathbb{Z},+,\cdot)$, $(\mathbb{R},+,\cdot)$

$M_2(\mathbb{R}) = \{ 2\times 2 \text{ matrices} \}$ $\quad$ ~~A+B~~

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}$$

---

if the ring has a mult. identity we call it 1

and say the ring is a "ring w/ identity"

$M_2(\mathbb{R})$ $\quad I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

ring w/ 1

if $\cdot$ is comm. in a ring then we say R is

a comm. ring.

comm. ring w/ 1 $\quad \mathbb{Z}, \mathbb{R}, \mathbb{Q}, \mathbb{C}$

3

~~$\mathbb{Z}$~~ $\underline{2\mathbb{Z}}$ comm. ring w/o 1.

$M_2(\mathbb{R})$ ring w/ 1 (non-comm.)

$\mathbb{Z}/n\mathbb{Z}$

$$[a]([b]+[c]) = [a]([b+c]) = [a(b+c)] = [ab+ac] = \; = [a][b]+[a][c]$$

$1=[1]$

$[1][a]=[a]$

$\underline{\text{Thm}}$ $\underline{\mathbb{Z}/n\mathbb{Z} \text{ is a comm. ring w/ } 1}$

we are looking for things that have mult. inverse.

these are called $\underline{\text{units}}$

$\underline{\text{Def}}$ 13 R ring w/ 1

$r \in R$ is a $\underline{\text{unit}}$ r is a

if $\exists\, s \in R$ s.t. $rs = sr = 1$

the set of units of R is denoted by $U(R)$

$$U(R) = \{x \in R \mid \exists\, y \in R \quad xy = yx = 1\}$$

$n>1$

$$U(n) := U(\mathbb{Z}/n\mathbb{Z}) = \{$$

$$U(6) = \{ [1],$$

4

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

$U(6) = \{[1], [5]\}$

$\mathbb{Z}/6\mathbb{Z}$

$[2][3] = [0]$

$[4][3] = [0]$

if $a, b \neq 0$.
but $ab = 0$
then $a \notin U(R)$.

if $ab = 0$ + a is unit

$b = 1 \cdot b = a^{-1}(ab) = a^{-1}0 = 0$

Thm $U(n) = \{[a] \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(a, n) = 1\}$.

$U(M_2(\mathbb{R})) = GL_2(\mathbb{R}) = \{A \in M_2(\mathbb{R}) \mid \det(A) \neq 0\}$

$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ $A^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

if R is a ring w/ 1, then $(U(R), \cdot, 1)$ is a group.

$u, v \in U(R)$ $(uv)^{-1} = v^{-1} \cdot u^{-1}$

Pf. $(v^{-1} \cdot u^{-1})(uv) = v^{-1}(u^{-1}u)v = v^{-1} \cdot 1 \cdot v = v^{-1}v = 1$

(5) $(G, *, e)$ $a, b \in G$.

$(ab)^{-1} = b^{-1}a^{-1}$ $(b^{-1}a^{-1})(ab) = e$.

<u>Def. 14</u> A <u>field</u> is a comm. ring w/ 1 F

so that $F \setminus \{0\} = U(F)$.

(every non-zero element has a mult. inv.).

<u>Ex</u> $\mathbb{R}, \mathbb{Q}, \mathbb{C}$

$\mathbb{Z}/p\mathbb{Z}$ (p prime)

<u>non-Exs</u> $\mathbb{Z}$

$M_2(\mathbb{R})$

$U(6)$

<u>Thm</u> $\mathbb{Z}/n\mathbb{Z}$ is a field iff $\forall\ 1 \le a \le n-1$, $\gcd(a,n) = 1$

iff

if n is prime then $\gcd(a,n) = 1$ or n so if $1 \le a < n$

$\gcd(a,n) = 1$

Conversely, if n not prime $\exists\ 1 < a < n$ $a \mid n$.

$\gcd(a,n) = a > 1$. so $\mathbb{Z}/n\mathbb{Z}$ <u>not a field</u>

(6) $\mathbb{Z}/5\mathbb{Z}$.

$[1]^{-1} = [1]$, $[-1]^{-1} = [-1]$

$[2]^{-1} = [3]$

$[3]^{-1} = [2]$

$\mathbb{Z}/7\mathbb{Z}$. $[2]^{-1} = [4]$ $[6]^{-1} = [6]$

$[3]^{-1} = [5]$

$\mathbb{Z}/11\mathbb{Z}$ $[2]^{-1} = [6]$ $[7]^{-1} = [8]$

$[3]^{-1} = [4]$ $[10]^{-1} = [10]$

$[5]^{-1} = [9]$

$\underline{\mathbb{Z}/10\mathbb{Z}}$ $\underline{[3]^{-1} = [7]}$

(7) Groups subgps $(G, *, e)$

$H \leq G$ $H \neq \emptyset$ $e \in H$, closed under $*$, inverses.

trivial $\{e\}$, G $H \leq G$

Ex $\mathbb{Z}$ $n\mathbb{Z} \leq \mathbb{Z}$

$(G, *, e)$ $g \in G$.

$$\langle g \rangle = \{g^k : k \in \mathbb{Z}\} = \{x \in G \mid \exists k \in \mathbb{Z} \ x = g^k\}$$

Note if we use addition $(G, +, 0)$

$$\langle g \rangle = \{kg \mid k \in \mathbb{Z}\}$$

Claim $\langle g \rangle \leq G$. $e = g^0$ $0 \in \mathbb{Z}$.

$x, y \in \langle g \rangle$ $\exists k, j \in \mathbb{Z}$ $x = g^k$, $y = g^j$

(subgp criterion) $xy^{-1} = g^k (g^j)^{-1} = g^k g^{-j} = g^{k-j} \in \langle g \rangle$. $k-j \in \mathbb{Z}$ ∎

~~This is~~ $\langle g \rangle$ is called the cyclic subgp generated by g.

8

$U(7) = \{1, 2, 3, 4, 5, 6\}$ mult

$\langle 2 \rangle = \{2, 4, 1\}$

$2^4 = 2^3 \cdot 2 = 2$

$2^{-1} = 4 = 2^2$

$2^{-2} = 4^2$

$(\mathbb{Z}, +, 0)$ $\{0\}$

$\langle 2 \rangle = \{2, 4, 6, 8, 10, \ldots\}$

$\cup \{-2, -4, -6, -8, \ldots\}$

$U(7)$

S_n

$\langle (123) \rangle = \{(123), (132), e\}$

$(123)(123) = (132)$

$(123)(132) = e.$

~~(abcde)~~

$$\boxed{(a_1 a_2 \ldots a_n)^{-1} = (a_1 a_n a_{n-1} \ldots a_2)}$$

$(1234)(1234) = \cancel{(12)}(13)(24)$

$(1234)(13)(24) = (1432)$

$\langle (1234) \rangle = \{e, (1234), (13)(24), (1432)\}$

$(1234)(1432) = e.$