①

In a ring with 1 an elt u is called a unit if it has a multiplikation inverse u^{-1}:

$$u^{-1}u = 1 = uu^{-1}$$

u "has two inverses" : $\begin{cases} u+(-u) = 0 \\ u^{-1}u = 1 = uu^{-1} \end{cases}$

$U(R) = \{u \in R \mid u \text{ a unit in } R\}$

is a group.

$U(\mathbb{Z}_n) = U(n)$

$U(\mathbb{Z}) = \{\pm 1\}$

$U(\mathbb{Q}) = \mathbb{Q} \setminus \{0\}$

Defⁿ A ring R is called a field if

- R a commutative ring
- R has $\underline{1}$
- Every $u \neq 0$ in is a unit.

Ex: $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_5$

Thm. Every finite integral domain is a field.

Pf: $D = \{0, 1, d_1, \ldots, d_n\}$

Products of d_1: $\underbrace{\{d_1, d_1^2, d_1 d_2, \ldots, d_1 d_n\}}_{D \setminus \{0\}}$

$$d_1 d_i = d_1 d_j$$
$$\Downarrow$$
$$d_1 (d_i - d_j) = 0$$
$$\Downarrow \text{ domain}$$
$$d_i - d_j = 0$$
$$\Downarrow$$
$$d_i = d_j$$

$\therefore$ 1 is among the elt.'s $d_1, d_1^2, d_1 d_2 .. d_1 d_n$

Corollary: $\mathbb{Z}_p$ is field if and only if p is prime.

(3)

Thm Every field is a domain.

Pf: Let $a \neq 0$ and assume $ab = 0$

Now $a^{-1}ab = a^{-1}0$

$b = 0.$ $\square$

Def^n If R is a field and $S \subseteq R$ is a field, then it is called a subfield of R.

Subfield test $S \subseteq R$, $S \neq 0$:

$a - b \in S$, $\forall a, b \in S$

$ab^{-1} \in S$, for $a, b \in S$, $b \neq 0$

Def^n A ring with 1 in which every $u \neq 0$ is a unit is called a division ring.

④ Def^n Let R be ring. The characteristic of R is the least $n \in \mathbb{N}$ such that $n \cdot a = 0$ for all $a \in R$. If no such n exists the char. is 0.

Ex $\operatorname{char} \mathbb{Z} = 0$

$\operatorname{char} \mathbb{Q} = 0$

$\operatorname{char} \mathbb{Z}_4 = 4$

$\operatorname{char} \mathbb{Z}_n = n$

Thm. Let R be a ring with 1. Then

(1) $\operatorname{char} R = 0$ if 1 has ∞ order under +

(2) $\operatorname{char} R = n$ if $|1| = n$ under +.

Pf: If $n \cdot 1 \neq 0$ for all $n \in \mathbb{N}$, then char 0.

If $|1| = n$, then $n \cdot a = n \cdot (1a)$
$= (n \cdot 1)a = 0a = 0.$

⑤ Thm. Let R be an integral domain. char R is 0 or p, for some prime p.

Pf Assume that char $R \neq 0$, i.e. char $R = n \in \mathbb{N}$. If n is not prime, then $n = ab$.

$n = |1|$. $\quad n \cdot 1 = 0$

$(ab) \cdot 1 = (a \cdot 1)(b \cdot 1) = 0$

$\therefore \quad a \cdot 1 = 0$ or $b \cdot 1 = 0$

$\therefore \quad a = n$ and $b = 1$.

⑥ $H = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$, $J = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, $K = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$

$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

$H^2 = -I$, $J^2 = -I$, $K^2 = -I$

$HJ = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} = K \qquad JH = \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix} = -K$

$HK = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = -J = -KH$

$JK = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} = H = KJ$

$\mathbb{H} = \{ aI + bJ + cK + dH \mid a, b, c, d \in \mathbb{R} \}$

$\subseteq \mathbb{C}_{2\times2}$ a subring

$h = aI + bJ + cK + dH \neq 0$

$h^* = aI - bJ - cK - dH$

$hh^* = (a^2 + b^2 + c^2 + d^2) I \neq 0$

$h^{-1} = \frac{1}{a^2 + b^2 + c^2 + d^2} h^*$

$\mathbb{H}$ is a division ring.