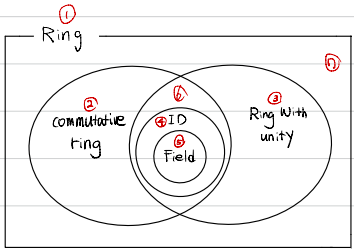
Q : field 구하는 과정.



ex)
① 생략.
② $2\mathbb{Z}$
③ $M_2(\mathbb{Z}_3)$
④ $\mathbb{Z}$
⑤ $\mathbb{Z}_p$
⑥ $\mathbb{Z}_6$
⑦

① Ring : $(R, +, \cdot)$

1. $(R, +) \rightarrow$ abelian group
2. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
3. $a(b+c) = ab + ac$, $(a+b) \cdot c = ac + bc$.

② commutative ring : ring 에서의 곱셈에 교환법칙 성립한 ring.

③ field : $(R, +, \cdot)$ 에서 Ring 이고, $(R-\{0\}, \cdot)$ 가 abelian group.

④ ID : commutative ring with no zero divisor (모든 원소에 대해 곱셈에 대한 역원이 존재)

⑤ unity : 곱셈항등원.

unit : 곱셈역원을 가지는 모든 원소들.

⑥ $(G, +)$ 가 abelian group.

① G가 덧셈에 대해 닫혀있고.
② 결합법칙이 성립.
③ 항등원이 존재.
④ 역원이 존재.
⑤ 교환법칙이 성립.

⑦ $(R-\{0\}, \cdot)$ is abelian group.

① $a \cdot b \in R-\{0\}$, $\forall a, b \in R-\{0\}$.
② 결합법칙 성립 : $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
③ 항등원이 존재. $e \in R-\{0\}$, $a \cdot e = e \cdot a = a$. $\forall a \in R-\{0\}$.
④ 역원이 존재. $a^{-1} \in R-\{0\}$, $a \cdot a^{-1} = a^{-1} \cdot a = e$
⑤ $a \cdot b = b \cdot a$.

① ② ③ ⑤ 는 자명하므로 ④만 증명.

⑧ sub ring , sub field -

정해진 ring의 부분집합을 뺐을 때 그 집합이 ring 이면 sub ring.

〃 field의 〃 . 〃 〃 field이면 sub field.

⑨ zero divisor 란

$a, b \neq 0$ 일때 $a \cdot b = 0$ 이 되게하는 a, b를 zero-divisor 라 한다.

ex) $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$.

$2 \cdot a = 0$ $a \neq 0$ $a = 3$.

$\therefore$ 2, 3은 zero divisor.

⑩ Char(R) 이 Ring with unity.

If $n \cdot 1 \neq 0$ for all $n \in \mathbb{Z}^+$ then $\text{char}(R) = 0$

If $n \cdot 1 = 0$ for all $n \in \mathbb{Z}^+$ then

$\text{char}(R)$ is smallest n

⑪ $\text{Char}(\mathbb{Z}) = 0$ $\text{Char}(\mathbb{Q}) = 0$. $\text{char}(R) = 0$.

$\text{char}(R_1 \times R_2)$ = GCD of $|R_1|$, $|R_2|$

$|R_1|$ 은 R_1의 원소가 하고 있는 개수를 의미한다.

ex) $\mathbb{Z}_5$, $\mathbb{Z}_{12}$ $\text{char}(\mathbb{Z}_5 \times \mathbb{Z}_{12})$

$\text{char}(\mathbb{Z}_5 \times \mathbb{Z}_{12}) = \{|\mathbb{Z}_5|, |\mathbb{Z}_{12}|\} = (5, 12) = 60$.

⑫ Little theorem of Fermat

$a^{p-1} \equiv 1 \pmod p$ for $a \neq 0 \pmod p$: a가 p로 나누어 떨어지지 않을 때 $a^{p-1} \div p$ 의 나머지는 1이다.

ex) $4^6 \equiv 1 \pmod 7$ $4^6 = 4^{n-1}$

⑬ $\mathbb{Z}_n^* = \{1, 2, 3, \cdots, n-1\}$.

ex) in $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$.

$\langle 2 \rangle = \{2, 4, 1\}$. (×2, ×2, ×2)

$\langle 3 \rangle = \{3, 6, 5\}$. (×3, ×3, ×3)