1. Groups, 군

군(group)의 정의

A group is a set G equipped with an binary operation * and a special element $e \in G$, called the identity, such that

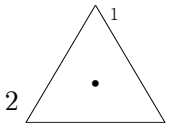
(1) the associative law holds: for every $a,b,c \in G$, $a * (b * c) = (a * b) * c$

(2) $e * a = a = a * e$ for all $a \in G$

(3) for every $a \in G$, there is $a' \in G$ with $a' * a = e = a * a'$

(1) Examples of groups

Example 1. 수체계가 아닌 Group의 예



정n각형의 rigid motion(강체운동)은 다각형의 중심을 고정한 회전이동과 대칭이동 모두 2n가지이다. Dihedral group D_n은 원소가 2n개이다.

정3각형에서 D_3은 예을 들어 120° 회전이동 : 1→2, 2→3, 3→1이다.

$$\rho_0 = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \quad \rho_1 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \quad \rho_2 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

$$\mu_1 = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}, \quad \mu_2 = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}, \quad \mu_3 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$$

$$\rho_1 \circ \mu_1 \neq \mu_1 \circ \rho_1$$

$\therefore D_3$: Abel group이 아니다.

Example 2.

X : set

Δ : symmetric difference

$A \Delta B = (A - B) \cup (B - A)$

$(B(X), \Delta)$: Boolean group

$(A \Delta B) \Delta C = A \Delta (B \Delta C)$: 벤다이어그램 이용

$A \Delta \phi = A$

$A \Delta A = \phi$

Example 3. Affine group

$(Aff(1, \mathbb{R}), \circ)$: group

① $f, g \in Aff(1, \mathbb{R}) \Rightarrow f \circ g \in Aff(1, \mathbb{R})$

② $(f \circ g) \circ h = f \circ (g \circ h)$

③ identity? $1_{\mathbb{R}}(x) = x$

④ f의 inverse?

Example 4. Stochastic group

$(\Sigma(2,\mathbb{R}),\times)$: group 여기서 연산은 행렬곱이다.

$A,\ B\in\Sigma(2,\mathbb{R}),\qquad A\times B\in\Sigma(2,\mathbb{R})$?

- $\det(A\times B)=\det(A)\det(B)$
- $\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}a' & b'\\ c' & d'\end{pmatrix}=\begin{pmatrix}aa'+bc' & ab'+bd'\\ ca'+dc' & cb'+dd'\end{pmatrix}$

$$(aa'+bc')+(ca'+dc')=(a+c)a'+(b+d)c'$$
$$=a'+c'=1$$
$$(ab+bd')+(cb'+dd')=(a+c)b'+(b+d)d'$$
$$=b'+d'=1$$

Associative law is holds

Identity : $\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$

$A^{-1}\in\Sigma(2,\mathbb{R})$

- $\det(A\times A^{-1})=\det(A)\det(A^{-1})=\det(E)=1$

$$\therefore\det(A^{-1})\neq 0$$

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

$$\frac{1}{ad-bc}(d-b)=1$$
$$\because a+b=1=c+d\ \Rightarrow\ ad-bc=(1-b)d-b(1-d)$$
$$=d-bd-b+bd=d-b$$

(2) Classification of group of order n

$(G,\ *)$: a group of $|G|=n$

①

$*$	e
e	e

②

$*$	e	a
e	e	a
a	a	e

ex1. $\mathbb{Z}_2=\{\bar{0},\ \bar{1}\},\oplus_2$

ex2. $\mathbb{R}^X\supset\{1,\ -1\},\ \times$

③

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

$a*a=a \Rightarrow a*a=a=a*e \Rightarrow a=e$ (모순)

④

*	e	a	b	c
e	e	a	b	c
a	a	(a)		
b	b		(b)	

(a)에 e가 들어가면, (b)에는 e또는 a.

(a)에 b또는 c가 들어가면 곱셈표가 완성된다.

Ⅰ. (a)$=e$, (b)$=e$: $a^2=b^2=c^2=e$

Ⅱ. (a)$=e$, (b)$=a$: $b^2=a$, $b^3=c$, $b^4=e$

Ⅲ. (a)$=b$: $a^2=b$, $a^3=c$, $a^4=e$

Ⅳ. (a)$=c$: $b^2=c$, $b^3=a$, $b^4=e$ Ⅱ, Ⅲ, Ⅳ는 cyclic 이고,

Ⅱ, Ⅲ 는 isomorphic 이다.

$\because \phi : G \to G$

$b \to \phi(b)=a$

$a \to b$

$c \to c$

따라서 $n=4$인 group은 $\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$로 2가지이다.

(3) Subgroups

Definition 1. subgroup

(G, $*$) : group

$H \subset G$, (H, $*$) 가 군 G와 같은 이항연산에 대하여 군이면 H를 G의 subgroup 이라한다.

Theorem 1.

G : a group

$H \subset G$

$H \leq G$, H가 G의 부분군 $\Leftrightarrow$ ① $\forall a,\ b \in H,\ a*b \in H$

② $\forall a \in H,\ a^{-1} \in H$

proof :

($\Leftarrow$) clear

($\Rightarrow$) • associative

$a,\ b,\ c \in H,\quad a*(b*c) = (a*b)*c \in G$

By ①, $a*(b*c) = (a*b)*c \in H$

• $e \in H$?

$\forall a \in H,\quad a^{-1} \in H$ (By ②)

$e = a*a^{-1} \in H$ (By ①)

Theorem 2.

G : group

$H \leq G \quad \Leftrightarrow \quad \forall a,\ b \in H,\quad a*b^{-1} \in H$

Example 5.

($\mathbb{Z}$, +) : a group

H : subgroup of $\mathbb{Z} \Rightarrow \exists n$ s.t. $H = n\mathbb{Z} = \{nr \mid r \in \mathbb{Z}\} = <n>$

proof :

Choose a least positive number n in H

i.e. $n = \min\{m \in H \mid m > 0\} \in \mathbb{N}$

$\exists n \in H \Rightarrow n\mathbb{Z} \subset H$

$\forall m \in H,\quad m = nq + r,\ 0 \leq r < n$ by division algorithm in $\mathbb{Z}$

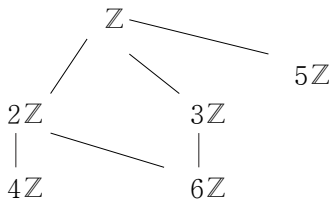
$\therefore\ r = m - nq \in H$

if $r > 0$, then n이 least positive number인것에 모순된다.

$\therefore\ r = 0$

즉, $\forall m \in H,\quad m = nq \in n\mathbb{Z} \quad \therefore H \subset n\mathbb{Z}$

$\therefore\ H = <n> = n\mathbb{Z}$



(4) Cyclic subgroups(순환군)

Definition 2.

G : group, $a \in G$

$<a>$: the cyclic subgroup of G generated by a

$<a>$: subgroup of G

$\because$ ① $\forall a^n,\ a^m \in <a>$

$$a^n \cdot a^m = a^{n+m} \in <a>$$

② $\forall a^n \in <a>$

$$(a^n)^{-1} = a^{-n} \in <a>$$

Note1. G : a group, $a,\ b \in G$

$$< a,b > = a^i b^j a^{-k} b^{-l}$$

G가 Abel. 이라면 $ab = ba$이므로, 원소를 위와 같이 쓸 필요가 없다.

Example 6.

$(\mathbb{Z}, +) \ni 4,\ 6$

$$< 4, 6 > = 4\mathbb{Z} + 6\mathbb{Z} = 2\mathbb{Z}$$

Note2. G : a group, $S \subset G$

$$< S > = \left\{ a_1^{i_1} a_2^{i_2} \cdots a_n^{i_n} \mid a_1, \cdots, a_n \in S,\ i_1, \cdots, i_n \in \mathbb{Z} \right\}$$

$$= \bigcap_{i \in \Gamma} G_i,\quad S \subset G_i \leq G$$

: 군 G에서 S를 품는 가장 작은 부분군이다.

:the smallest subgroup of G containing S

proof :

$\forall i,\ (A) \subset G_i$ where $S \subset G_i \leq G$

$\because\ a_1^{i_1}, \cdots,\ a_n^{i_n} \in (A)$ for *all* $a_1, \cdots, a_n \in S \subset G_i,\ i_1, \cdots, i_n \in \mathbb{Z}$

Note3.

① $(\mathbb{Z}, +) <$ $\begin{matrix} 2\mathbb{Z} = \overline{0} \\ 2\mathbb{Z}+1 = \overline{1} \end{matrix}$

$\{\overline{0},\ \overline{1}\} = \mathbb{Z}_2,\ \oplus_2$: a group

② $(\mathbb{Z}, +) \ni n$

$$\begin{matrix} n\mathbb{Z}, & n\mathbb{Z}+1, & \cdots, & n\mathbb{Z}+(n-1) \\ \| & \| & & \| \\ \overline{0} & \overline{1} & & \overline{n-1} \end{matrix}$$

$\{\overline{0},\ \overline{1}, \cdots, \overline{n-1}\} = \mathbb{Z}_n,\ \oplus_n$: group

Definition 3. $a \equiv_n b$ is an relation in $\mathbb{Z}$

$$\Leftrightarrow\ \forall a, b \in \mathbb{Z},\ a - b = nZ \text{ for some n in } R$$

then $\equiv_n$ is an equivalence relation on $\mathbb{Z}$

$$a \equiv_n a$$

$$a \equiv_n b \Rightarrow b \equiv_n a$$

$a \equiv_n b$ and $b \equiv_n c \Rightarrow a \equiv_n c$

: equivalence class of a

$a/\equiv_n = \{b \mid a \equiv_n b\} = a + n\mathbb{Z}$

$\because\ b - a = nZ,\ \ b = a + nZ$

Hence

$$\mathbb{Z}/\equiv_n = \{n\mathbb{Z},\ n\mathbb{Z}+1, \cdots,\ n\mathbb{Z}+(n-1)\} = \{\bar{0},\ \bar{1}, \cdots,\ \overline{(n-1)}\}$$

Then $\mathbb{Z}/\equiv_n$: group ?

$\because\ \bar{a},\ \bar{b} \in \mathbb{Z}_n$

① $\bar{a} \oplus_n \bar{b} = \bar{c} \in \mathbb{Z}_n$ where $a + b = nZ + c,\ n = 0$ or $1,\ 0 \le c < n$

② $\bar{0}$: identity

③ $\bar{a} \oplus \overline{(n-a)} = \bar{0}$

Definition 4.

G : group

$\exists\, a \in G\ \ s.t.\ \ < a >= G\ \Rightarrow\ \ G$: cyclic group

Theorem 3.

Any cyclic group is isomorphic to $\mathbb{Z}$ or $\mathbb{Z}_n$

proof : G : cyclic $\Rightarrow\ \exists\, a \in G\ \ s.t.\ \ < a >= G$

i) G : finite

$|G| = n$

$$|G| = n\ \Rightarrow\ \exists\, i \neq j\ \ s.t.\ \ a^i = a^j$$

$$\Rightarrow i > j,\ \ a^{i-j} = e$$

$m = \min\{R \mid a^R = e\} \subset \mathbb{N}$ 라 하면,

$|G| = n$ 이므로, $m = n$

$\therefore\ (G, *) \cong (\mathbb{Z}_n, \oplus_n)$

ii) G : infinite $\Rightarrow\ \forall i \neq j,\ \ a^i \neq a^j$

$\Rightarrow\ G = \{a^n \mid n \in \mathbb{Z}\} \cong \mathbb{Z}$

Theorem 4.

Any Abel group is isomorphic to $\mathbb{Z}^n \times \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$

Theorem 5.

Any finite Abel group is isomorphic to $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$

(5) Permutation groups

Permutation groups

① X : set

$S_X = \{\sigma : X \to X : bijection\}$

$(S_X, \circ)$: symmetric group of permutations

② $|X| = n$

$X = \{1, 2, \cdots, n\}$

$S_n \ni \sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$

$|S_n| = n!$

Definition. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 3 & 4 & 6 & 1 & 8 & 7 & 2 \end{pmatrix} = (1\ 5)(2\ 3\ 4\ 6\ 8)(7)$

$\therefore$ {1, 2, 3, 4, 5, 6, 7, 8} 은 {1, 5}, {2, 3, 4, 6, 8}, {7}로 분할할 수 있다.

$\sigma = (1\ 5)(2\ 3\ 4\ 6\ 8)$

③ 모든 cycle은 disjoint cycle의 곱으로 쓸 수 있다.

④ cycle은 호환들의 곱으로 쓸 수 있다.

$(2\ 3\ 4\ 6\ 8) = (2\ 8)(2\ 6)(2\ 4)(2\ 3)$

$\therefore\ \sigma = (1\ 5)(2\ 8)(2\ 6)(2\ 4)(2\ 3)$ 은 호환의 개수가 기수이므로 기순열이다.

⑤ 행렬식의 정의

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} = \sum_{\sigma \in S_n} sgn(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)})$$

(6) Lagrange's theorem

Definition 5. G : a group, $H \leq G$, a, $b \in G$

$a \sim_H b \Leftrightarrow a^{-1}b \in H$

Then $\sim_H$ is an equivalence relation

$\because$ ① $a \sim_H a$

② $a \sim_H b \Rightarrow b \sim_H a$

($\because$ $a^{-1}b \in H$, H : group $\Rightarrow$ $(a^{-1}b)^{-1} = b^{-1}a \in H$)

③ $a \sim_H b$, $b \sim_H c \Rightarrow a \sim_H c$

Hence

$a/\sim_H = \{b \in G \mid a^{-1}b \in H\} = \{b \in G \mid b = ah\} = aH$

equivalence class of a

$G/\sim_H = G/H$ 로 쓰기로 약속한다.

그러면, $G = \dot{\bigcup}_{a \in G} aH$: a partition of G

$\because$ ① $\bigcup_{a \in G} aH \subset G$, $\bigcup_{a \in G} aH \supset G$ ($\because x \in G$, $x = x \cdot e \in xH$)

$\therefore \bigcup aH = G$

② aH들은 disjoint이다. ($aH \cap bH \neq \varnothing \Rightarrow aH = bH$)

$c \in aH \cap bH$

then $c \in aH$ and $c \in bH$

$\Rightarrow a \sim_H b$ and $c \sim_H b$

$\therefore a \sim_H b \Rightarrow b \in aH \Rightarrow bH \subset aH$

또한 $c = ah_1$, $c = ah_2$ 이다.

$$\forall x \in aH, \quad x = ah = (ch_1^{-1})h = c(h_1^{-1}h) = (bh_2)(h_1^{-1}h)$$

$$= b(h_2 h_1^{-1}h) \in bH$$

$\therefore aH \subset bH$

한편, $|H| = |aH|$, $\forall a \in G$

$\because f : H \to aH$

$x \to f(x) = ax$

- f : map ($\because$이항연산이므로 함수가 된다.)
- 1-1 ($\because ax = ay \Rightarrow x = y$, group의 소약법칙)
- onto

Theorem 6.

G :a finite group, $H \leq G$

$G = \bigcup_{a \in G} aH = a_1 H \cup \cdots \cup a_n H$

$|H| = |aH|$

Hence, $|G| = n|H|$, n : the number of cosets

이때, n : the index of H in G

$n = i n_G(H) = (G : H)$

따라서, $|H| \mid |G|$

Example 7. ① $\{0, 1, 2, 3, 4, 5\}$, $\oplus_6$

$\{0, 1, 2, 3\} \not\leq \mathbb{Z}_6$

이고, $\{0, 3\} \leq \mathbb{Z}_6$

② $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$, $\oplus_5$

$\mathbb{Z}_5$의 $\{0\}$ 이외의 subgroup은 없다.

Theorem 7.

$|G| = p$, p : prime

$\Rightarrow G = \langle a \rangle$ for some nonidentity a in G

proof :

$a \in G$, $<a>$: a cyclic subgroup of G

But $|G| = p$, $|<a>| \mid p$

Hence $|<a>| = p$

$\therefore <a> = G$

원소 개수의 측면에서

$n = 4$: $\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$

$n = 6$: $\mathbb{Z}_6$, S_3

$n = 8$: $\mathbb{Z}_8$, $Z_2 \times \mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, D_4, Q_4

Note; 일반적으로 Lagrange's theorem 의 역은 성립하는가?

G : a group, $|G| = n$

$m \mid n \Rightarrow \exists H \leq G$ s.t. $|H| = m$?

반례 : A_4

$|A_4| = 12$ and $6 \mid 12$ but $\nexists H \leq A_4$ s.t. $|H| = 6$

(7) Normal subgroups

G is a group and H is a subgroup of G

$\{aH \mid a \in G\}$ 에서

이항연산 $(aH) * (bH) = abH$ 은 잘 정의되는가?

$* : G/H \times G/H \rightarrow G/H$: map 인가?

$(aH, bH) \rightarrow abH$

$(a'H, b'H) \rightarrow a'b'H$ 일 때

(aH,bH)=(a'H,b'H) 이면 $abH = a'b'H$ 인가?

$aH = a'H \Rightarrow a \sim_H a' \quad \therefore a^{-1}a' \in H$

$bH = b'H \Rightarrow b \sim_H b' \quad \therefore b^{-1}b' \in H$

$ab \sim_H a'b'$? $\quad (ab)^{-1}a'b' = b^{-1}a^{-1}a'b' \in H$?

따라서 $aH = Ha$ 이 성립하면 곱을 정의할수 있겠다는 생각을 하게된다.

Example 8.

$S_3 = \{\rho_0, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3\}$

$H = \{\rho_0, \mu_1\}$

$S_3/H = \{H, \rho_1 H, \rho_2 H\}$

$\rho_1 H = \{\rho_1, \mu_3\} \neq \{\rho_1, \mu_2\} = H\rho_1$

Definition 6.

G : group, $H \leq G$

H : a normal subgroup of $G \Leftrightarrow \forall a \in G,\ aH = Ha$

Example 9.

$H = \{\rho_0, \mu_1\}$: not normal subgroup of S_3

$K = \{\rho_0, \rho_1, \rho_2\}$: normal subgroup of S_3

$\mu_1 K = \{\mu_1, \mu_2, \mu_3\} = K\mu_1$

Theorem 8.

G : Abel. group

$\forall H \leq G,\ H$: normal

proof :

$a \in G \Rightarrow ah = ha \in Ha$

Theorem 9.

G : a group, $H \leq G$

Then the followings are equivalent.

① $\forall a \in G,\ aH = Ha$

② $\forall a \in G,\ aH \subset Ha$

③ $\forall a \in G,\ H \subset a^{-1}Ha$

④ $\forall a \in G,\ \forall h \in H,\ h \in a^{-1}Ha$

proof : ② ⇒①

$\forall h \in H$,

$a^{-1} \in G \Rightarrow a^{-1}H \subset Ha^{-1} \Rightarrow a^{-1}h \in Ha^{-1} \Rightarrow a^{-1}h = h'a^{-1}$ for some $h' \in H$

$\Rightarrow ha = ah' \in aH \quad \therefore Ha \subset aH \quad \therefore Ha = Ha$

Theorem 10.

G : group, $H \lhd G,\ G/H = \{aH \mid a \in G\}$

$\Rightarrow (G/H, *)$: group

proof :

① $*$: 이항연산

② Assocative.

③ 항등원 : $eH = H$

$\because eH \cap H \ni e$ 즉, $eH \cap H \neq \varnothing \Rightarrow eH = H$

④ 역원 : $(aH)^{-1} = a^{-1}H$

$\because (aH)(a^{-1}H) = aa^{-1}H = eH = H$

$(G/H, *)$: quotient group

Example 10. S_3/K : quotient group $\cong \mathbb{Z}_2$

Theorem 11.

G : finite group, $H \lhd G$, G/H : factor group

$\Rightarrow |G/H| = (G:H) = |G|/|H|$

hence $|G| = (G:H)\,|H|$

Theorem 12.

G : group, $|G| = 2n$, $H \leq G$, $|H| = n$

$\Rightarrow H \lhd G$

proof :

$\forall a \in G$

i) $a \in H \Rightarrow aH = H$

ii) $a \notin H \Rightarrow G = H \dot{\cup} aH = H \dot{\cup} Ha$

$\therefore aH = Ha$

Example 11.

$S_n \geq A_n$: 교대군 (Alternating group)

$\Rightarrow A_n \lhd S_n$

Example 12. A_4의 원소의 개수가 6개인 subgroup은 없다.

$|A_4| = 12,\ 6 | 12$

원소가 6개인 subgroup H가 있다면,

$H \lhd A_4 \Rightarrow \{H, \sigma H\}$, $\sigma \notin H$

$(\sigma H)(\sigma H) = \sigma^2 H = H \Rightarrow \sigma^2 \in H$

but $\sigma = (1\,2\,3) \in A_4$ 라면, $\sigma^2 = (1\,2\,3)(1\,2\,3) = (1\,3\,2) \in H$

$(\sigma^2)^2 = (1\,3\,2)^2 = (1\,2\,3) \in H$ 즉, $\sigma \in A_4 \Rightarrow \sigma^2 \in H$ 이다.

이와 같은 방법으로 계산하면,

$\{(1\,2\,3), (1\,3\,2), (1\,2\,4), (1\,4\,2), (1\,3\,4), (1\,4\,3), (2\,3\,4), (2\,4\,3)\} \subset H$

$\Rightarrow |H| \geq 8$

(8) Group homomorphism(군 준동형사상)

Definition 7.

$\varphi : G \rightarrow G'$: map $s.t.$ $\varphi(a * b) = \varphi(a) * \varphi(b)$

$\Rightarrow \varphi$: a group homomorphism from G to G'

Example 13.

① $f : \mathbb{Z} \rightarrow \mathbb{Z}$, $f(x) = 2x$:a homomorphism

② $f(x) = x^2$: not a homomorphism

③ $f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$, $f(x) = x^p$: a homomorphism

$\because f(x+y) = (x+y)^p = x^p + y^p = f(x) + f(y)$

④ $\exp : (\mathbb{R}, +) \rightarrow (\mathbb{R}^+, \cdot)$, $\exp(x) = e^x$: a homomorphism

$\because\ \exp(x+y)=e^{x+y}=e^{x}\cdot e^{y}=\exp(x)\cdot\exp(y)$

Basic property of a group homomorphism

$\varphi:\ G\to G'$: a group homomorphism.

Then ① $\varphi(e)=e'$

② $\varphi(a)^{-1}=\varphi(a^{-1})$

③ $H\leq G\ \Rightarrow \varphi(H)\leq G'$

④ $H'\leq G'\ \Rightarrow \varphi^{-1}(H')\leq G$

⑤ $H\lhd G\ \Rightarrow \varphi(H)\lhd\varphi(G)$

⑥ $H'\lhd G'\ \Rightarrow \varphi^{-1}(H')\lhd G$

proof :

① $\varphi(e)=\varphi(ee)=\varphi(e)\varphi(e)\ \Rightarrow\ \phi(e)=e'$

② $\varphi(a)\varphi(a^{-1})=\varphi(aa^{-1})=\varphi(e)=e'\qquad\therefore\ \varphi(a)^{-1}=\varphi(a^{-1})$

③ $\varphi(H)=\{\varphi(h)\mid h\in H\}$

$\forall\,\varphi(h),\ \varphi(h')\in\varphi(H)$

- $\varphi(h)\varphi(h')=\varphi(hh')\in\varphi(H)$
- $\varphi(h)^{-1}=\varphi(h^{-1})\in\varphi(H)$

$\therefore\ \varphi(H)\leq G'$

④ $\varphi^{-1}(H')=\{a\in G\mid\varphi(a)\in H'\}$: inverse image

$a\in\varphi^{-1}(H)\ \Leftrightarrow\varphi(a)\in H'$

- $a,\ b\in\varphi^{-1}(H')\ \Rightarrow\varphi(a),\ \varphi(b)\in H'\ \Rightarrow\varphi(ab)=\varphi(a)\varphi(b)\in H'$
- $a\in\varphi^{-1}(H')\ \Rightarrow\varphi(a)\in H'\ \Rightarrow\varphi(a^{-1})=\varphi(a)^{-1}\in H'$

$\therefore\ \varphi^{-1}(H')\leq G$

⑤ $\varphi(H)\leq\varphi(G)\leq G'$

for $\varphi(h)\in\varphi(H),\ \varphi(g)\in\varphi(G)$

$\varphi(g)\varphi(h)\varphi(g)^{-1}=\varphi(ghg^{-1})\in\varphi(H)$

⑥ $\varphi^{-1}(H')\leq G$

for $a\in\varphi^{-1}(H'),\ g\in G$

$\varphi(gag^{-1})=\varphi(g)\varphi(a)\varphi(g)^{-1}\in H'$ 즉, $gag^{-1}\in\varphi^{-1}(H')$

Theorem 13.

$\varphi:\ G\to G'$: homomorphism

φ : 1-1 $\Leftrightarrow\ker\varphi=\varphi^{-1}(e')=\{a\in G\mid\varphi(a)=e'\}=\{e\}$

proof :

$(\Rightarrow)\ \forall\,x\in\ker\varphi,\ \varphi(x)=e'=\varphi(e)$

since f : 1-1, $x=e$

$(\Leftarrow)\ \varphi(x)=\varphi(y)\ \Rightarrow\varphi(x)\varphi(y)^{-1}=e'\ \Rightarrow\varphi(xy^{-1})=e'$

$\Rightarrow\varphi(xy^{-1})=e'\ \Rightarrow xy^{-1}\in\ker\varphi=\{e\}$

$\therefore\ xy^{-1}=e,\quad x=y$

Example 14. $\exp : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$

$\ker(\exp) = \{r \in \mathbb{R} \mid \exp(r) = e^r = 1\} = \{0\}$ $\quad\therefore$ exp : 1-1

(9) The fundamental theorem of groups

$\phi : G \to G'$: group homomorphism.

$\ker\phi = K \lhd G$

lemma. G : a group

$H \lhd G \Rightarrow \phi : G \to G/H$, $\phi(a) = aH$: the natural homomorphism.

Then • $\exists \phi^* : G/K \to G'$: map $s.t.$ $\phi^*(aK) = \phi(a)$

• ϕ^* : a homomorphism, 1-1

Example 15.

$\phi : (\mathbb{R}, +) \to (\mathbb{C}, \cdot)$, $\phi(x) = e^{ix}$: a homomorphism.

$\ker\phi = \{x \in \mathbb{R} \mid e^{ix} = 1\} = <2\pi>$

$\mathbb{R}/<2\pi> = \{a + <2\pi> \mid a \in [0, 2\pi)\} \cong [0, 2\pi)$

$\phi(\mathbb{R}) = \{e^{ix} \mid x \in \mathbb{R}\}$: 중심이 (0, 0)이고, 반지름이 1인 circle이다.

또한, $\mathbb{R}/<2\pi>$와 $\phi(\mathbb{R})$는 위상적으로도 동형이다.

Proof of Fundamental Theorem.

Step1. $\phi^*(aK) = \phi(a)$: well-defined

$aK = bK \Rightarrow ab^{-1} \in K = \ker\phi$

$\Rightarrow \phi(ab^{-1}) = e'$

$\Rightarrow \phi(a)\phi(b)^{-1} = e'$ $\quad\therefore \phi(a) = \phi(b)$

Step2. ϕ^* : a homomorphism.

$\phi^*(aK\ bK) = \phi^*(abK) = \phi(ab) = \phi(a)\phi(b) = \phi^*(aK)\phi^*(bK)$

Step3. ϕ^* : 1-1 즉, $\ker\phi^* = \{aK \in G/K \mid \phi^*(aK) = e'\} = \{K\}$

$\phi^*(aK) \in \ker\phi^* \Rightarrow \phi(a) = \phi^*(aK) = e' \Rightarrow a \in \ker\phi = K$

Example 16.

① $\phi : \mathbb{Z}_{12} \to \mathbb{Z}_5$:a homomorphism

homomorphism ϕ가 존재한다면,

$\mathbb{Z}_{12}/\ker\phi \cong im\phi \leq \mathbb{Z}_5$

$12/a = 5$가 될 수는 없으므로, ϕ : a trivial homomorphism

② $\phi : \mathbb{Z}_{12} \to \mathbb{Z}_4$, $\ker\phi = \{0, 4, 8\}$

Definition 8.

$G_1 \times G_2 = \{(a_1, a_2) \mid a_1 \in G_1,\ a_2 \in G_2\}$:the direct product of G_1 and G_2

Note.

$\mathbb{Z}_2\times\mathbb{Z}_3=\{(0,0),\ (0,1),\ (0,2),\ (1,0),\ (1,1),\ (1,2)\}$

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

이 두 군이 동형임을 보이자.

sol.

$\mathbb{Z}_6=\mathbb{Z}/6\mathbb{Z}$임을 착안하여,

Define $\phi:\mathbb{Z}\to\mathbb{Z}_2\times\mathbb{Z}_3,\ \phi(n)=([n]_2,[n]_3)$

Then ϕ : function. ϕ : homomorphism.

ϕ : onto. $\ker\phi=6\mathbb{Z}$

Theorem 14.

$m,\ n$: 서로 소 $\Rightarrow\ \mathbb{Z}_m\times\mathbb{Z}_n\cong\mathbb{Z}_{m\times n}$

Proof :

define $\phi:\mathbb{Z}\to\mathbb{Z}_m\times\mathbb{Z}_n,\ \varphi(a)=([a]_m,[a]_n)$

then ϕ : homomorphism. onto. $\ker\phi=mn\mathbb{Z}$, where $(n,m)=1$

ϕ : onto 를 보이기 위해서는 다음을 보여야 한다.

$(b_1,b_2)\in\mathbb{Z}_m\times\mathbb{Z}_n$에 대해서 $x\equiv b_1\pmod m$, $x\equiv b_2\pmod n$인 x가 존재하는가? CRT.(page 69)

Lemma. $(a,m)=1\ \Rightarrow\ ax=b\pmod m$ has a solusion.

$\because\ (a,m)=1\ \Rightarrow\ ak_1+mk_2=1\ \Rightarrow\ ak_1\equiv1\pmod m$

$\Rightarrow$ a의 역원이 존재

$\therefore\ ax\equiv b\pmod m$의 해가 존재.

Another proof;

$\mathbb{Z}_{m\times n}=<1>$ 임에 착안하여

$<(1,1)>=\{(1,1),(2,2),\cdots,(0,m),(1,m+1),\cdots,(n-m,0),\cdots,(0,0)\}$

$|<(1,1)>|=mn$

$<(1,1)>\le\mathbb{Z}_m\times\mathbb{Z}_n\ \Rightarrow\ <(1,1)>=\mathbb{Z}_m\times\mathbb{Z}_n\cong\mathbb{Z}_{m\times n}$

Hence

$\mathbb{Z}_3\times\mathbb{Z}_4\cong\mathbb{Z}_{12}$

$\mathbb{Z}_2\times\mathbb{Z}_2\ncong\mathbb{Z}_4$ ($\because\ \mathbb{Z}_2\times\mathbb{Z}_2$ not cyclic, $\mathbb{Z}_4$: cyclic)

Definition 9. Isomorphism of groups

$G,\ G'$: group

$\varphi:\ G\to G'$: a homomorphism, bijection

$\Rightarrow\varphi$: an isomorphism from G to G'

Example 17.

① $(\mathbb{Z},+)$: a group

$\mathbb{Z}$에서 $\mathbb{Z}$로의 isomormorphism은 몇가지 있는가?

$\varphi : \mathbb{Z} \to \mathbb{Z}$, $\varphi(a) = na$

$\varphi(a+b) = \varphi(a) + \varphi(b)$

$\ker\varphi = \{0\}$

onto가 성립해야 함으로 $n = 1, \ -1$이어야 한다.

$\therefore$ isomormorphism은 2가지 뿐이다. $(\varphi(1) = 1, \ \varphi(1) = -1)$

② $\varphi : \mathbb{C} \to \mathbb{C}$, $\varphi(a+bi) = a - bi$

group homomorphism의 의미는 $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$와 같다.

Note.

G : the set of all groups

$\cong$: isomorphism

then $\cong$ is an equivalence relation

$\because \ G_1 \cong G_1 \ (1_G)$

$\varphi : G_1 \cong G_2 \ \Rightarrow \varphi^{-1} : G_2 \cong G_1$

$\varphi : G_1 \cong G_2, \ \psi : G_2 \cong G_3 \ \Rightarrow \psi \circ \varphi : G_1 \cong G_3$

그러므로 G는 up to isomorphism (동형의 관점에서) 분류할 수 있다.

어떤 군들이 동형이라는 뜻은 대수적 구조가 같다는 뜻이다.

$(\mathbb{Q}, +) \ncong (\mathbb{R}, +)$: order가 다르다.

$(\mathbb{C}^*, \cdot) \ncong (\mathbb{R}^*, \cdot)$

$order(i) = 4$ 이고, $\mathbb{R}^*$안에는 *order*가 4인 원소가 없다.

Theorem15.

군 G의 부분군 H와 정규부분군 N에 대하여 $(HN/N) \cong H/(H \cap N)$이 성립한다.

Theorem16.

군 G의 두 정규부분군 H, K에 대하여 $K \leq H$이면

$G/H \cong (G/K)/(H/K)$이 성립한다.

<연습문제>

1. Let G be a group with the following property: Whenever a, b and c belong to G and $ab = ca$, then $b = c$. Prove that G is Abelian.

2. In a finite group, show that the number of nonidentity elements that satisfy the equation $x^5 = e$ is a multiple of 4.

3. Let $H = \{ a + bi \mid a, b \in \mathbb{R}, \ ab \geq 0 \}$, prove or disprove that H is a subgroup of $\mathbb{C}$ under addition.

4. Let G be a finite group with more than one element. Show that G has an element of prime order.

5. Let $\beta = (1\ 2\ 3\ )(1\ 4\ 5)$, write β^{99} in disjoint cycle form.

6. If $\beta \in S_7$ and $|\beta^3| = 7$. prove that $|\beta| = 7$.

7. Prove or disprove that $U(20)$ and $U(24)$ are isomorphic.

8. In $Aut(\mathbb{Z}_9)$, let α_i denote the automorphism that sends 1 to i where $\gcd(i, 9) = 1$. Write α_5 and α_8 as permutations of $\{0, 1, ..., 8\}$ in disjoint cycle form.

9. The group $S_3 \oplus Z_2$ is isomorphic to one of the following groups :
   Z_{12}, $Z_6 \oplus Z_2$, A_4, D_6. Determine which one by elimination.

10. Let H be a subgroup of G and let $a, b \in G$.
    show that $aH = bH$ if and only if $Ha^{-1} = Hb^{-1}$.

2. Ring, 환

환(Ring)의 정의

R : a set

① $(R, +)$: an Abelian group

② $(R, \cdot)$: a semi group

③ distributive law

$\Rightarrow$ $(R, +, \cdot)$: Ring

(1) Examples of rings

Example 1.

$(\mathbb{Z}, +, \cdot)$: 정수환 (integers)

① $(\mathbb{Z}, +)$: Abelian group

② $(\mathbb{Z}, \cdot)$: semi group (closed, associative law)

③ $c(a+b) = ca + cb$: left distributive law

$(a+b)c = ac + bc$: right distributive law

덧셈, 곱셈 두기지 이항연산이 정수집합 안에서 공존한다는 의미를 갖는다.

Example 2.

$\mathbb{Z}[x] = \{ a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \mid a_i \in \mathbb{Z} \}$

$(\mathbb{Z}[x], +, \cdot)$: 다항식 환

Example 3.

$$M_n(\mathbb{R}) = \left\{ A \mid A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ \cdots & \cdots & a_{nn} \end{pmatrix}, \ a_{ij} \in \mathbb{R} \right\}$$

$(M_n(\mathbb{R}), +, \cdot)$:n차 행렬 환

Example 4.

$C[0,1] = \{ f \mid f : [0,1] \to \mathbb{R}, \ continuous \ function \}$

$f, \ g \in C[0,1], \quad (f \cdot g)(x) = f(x) \cdot g(x)$

$(C[0,1], +, \cdot)$: 함수 환

(2) Basic properties of a ring

$(R, +, \cdot)$: a ring

Then

① $0 \cdot a = 0 = a \cdot 0, \quad \forall a \in R$

$\because \ 0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a \ \Rightarrow \ 0 = 0 \cdot a$

② If R has a multiplicative unity 1, then $(-1)(-a) = a, \quad \forall a \in R$

$\because \ (-1)(-a) + (-a) = (-1)(-a) + 1(-a)$

$= ((-1)+1)(-a) = 0(-a) = 0$

③ $(-1)a = -a, \quad \forall a \in R$

$\because \ (-1)a + a = (-1)a + 1a = ((-1)+1)a = 0a = 0$

④ $(-a)b = -ab = a(-b), \quad \forall a, \ b \in R$

$\because \ (-a)b + ab = ((-a)+a)b = 0b = 0$

$(-a)(-b) = ab, \quad \forall a, \ b \in R$

$\because \ (-a)(-b) = -(a(-b)) = -(-ab) = ab$

Definition 2.

R : a ring, $S \subset R$

S is also a ring with the same operation in R

$\Rightarrow$ S is called a subring of R

Example 5.

① $\mathbb{Z} \supset 2\mathbb{Z}$: 부분환

② $M_2(\mathbb{R}) \supset \left\{ \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \mid a, \ c \in R \right\}$

③ $C(0,1) \supset D(0,1)$: differentiable functions.

Theorem 1.

R : a ring, $S \subset R$

S : a subring of $R \ \Leftrightarrow$

① $a, \ b \in R \ \Rightarrow \ a + (-b) \in R$ 즉, $S \leq R$(subgroup)

② $a, \ b \in R \ \Rightarrow \ ab \in S$

proof :

($\Leftarrow$) (1) $(S, +)$:an Abelian group

$0 = a + (-a) \in S$

$-a = 0 + (-a) \in S$

$a + (-(-b)) \in S$

$a + b = b + a$ in $R \ \Rightarrow \ a + b = b + a$ in S

(2) $(S, \cdot)$: semi group

(3) distributive law

Example 6.

$\mathbb{Z}[i] = \{ a + bi \mid a, \ b \in \mathbb{Z} \}$: Gaussian integer

$\mathbb{Z} \subset \mathbb{Z}[i] \subset \mathbb{C}$: subring의 관계

(3) Ideals

Definition 3.

R : a ring, I : a subring of R

$\forall a \in I$, $\forall r \in R \Rightarrow ar \in I$, $ra \in I$ 일 때

Then I is called a ideal of R

Example 7.

$\mathbb{Z} \supset 2\mathbb{Z} \supset 4\mathbb{Z} \supset 8\mathbb{Z} \supset \cdots$

$n\mathbb{Z}$는 $\mathbb{Z}$의 ideal

ideal이 많다. 이들의 연산은 어떻게 될까?

Theorem 2.

R : ring, $I \subset R$

I : ideal of $R \Leftrightarrow$ ① $\forall a, b \in I, \quad a-b \in I$

② $\forall a \in I, r \in R, \quad ar \in I, ra \in I$

Theorem 3.

I, J : ideal of $R \Rightarrow I \cap J$: ideal of R

Example 8.

$\mathbb{Z}$: ring, $12\mathbb{Z}$, $8\mathbb{Z}$: ideal of $\mathbb{Z}$

$12\mathbb{Z} \cap 8\mathbb{Z} = ?$

$12\mathbb{Z} \cap 8\mathbb{Z}$는 ideal이므로 group Z 안에서 찾아야 한다.

$12\mathbb{Z} \cap 8\mathbb{Z} = 24\mathbb{Z}$

$12\mathbb{Z} + 8\mathbb{Z} = 4\mathbb{Z}$

일반적으로

$n\mathbb{Z} \cap m\mathbb{Z} = lcm(n,m)\mathbb{Z}$

$n\mathbb{Z} + m\mathbb{Z} = \gcd(n,m)\mathbb{Z}$

다음부터는 환 R은 commutative ring 이고 곱셈에 대한 항등원 1를 갖는 경우만 생각하기로 한다.

Definition 4.

R : commutative ring with 1, I, J : ideal of R

$\Rightarrow I : J = \{a \in R \mid aJ \subset I\}$: ideal of quotient

$\sqrt{I} = \{a \in R \mid a^n \in I \text{ for } some\ n > 0\}$: radical of I

$\sqrt{I}$: ideal

$\because a, b \in \sqrt{I}$, $a^n, b^m \in I$

$(a-b)^{n+m} = a^{n+m} - {}_{(n+m)}C_1 a^{(n+m-1)}b + \cdots + (-1)^{n+m}b^{n+m}$

$r \in R, \quad (ra)^n = r^n a^n \in I$

$I+J$의 구체적 의미(Constructive meanning)은 무엇일까?

사실상 $I+J=<I \cup J>$:the smallest ideal of R containing I and J

Theorem 4.

R : a commutative ring with 1 , $S \subset R$

$<S>$: the ideal generated by S is equal to the smallest ideal of R containing S

즉, $A=\bigcap_{i=1} I_i$, $S \subset I_i$: ideal of R , $B=\left\{ \sum^{finite} s_i r_i \,\middle|\, s_i \in S,\ r_i \in R \right\}$

$\Rightarrow \ A=B$

proof :

B : ideal of R containing S

$\because \ \forall s \in S, \quad s=s \cdot 1 \in B \quad \therefore \ S \subset B$

and B : ideal

$\therefore \ A \subset B$

$\forall \sum s_i r_i \in B, \quad s_i \in S \subset I_i$ (I_i : i ideal)

$\therefore \ \sum s_i r_i \in I_j$

$\therefore \ B \subset I_i, \quad \forall i$

$\therefore \ B=A=\bigcap I_i$

$I+J=<I \cup J \geqq \bigcap i_i, \quad I \cup J \subset I_j$: ideal of $R, \quad \forall i$

Example 9.

$I=12\mathbb{Z}$, $J=18\mathbb{Z}$ 일때

$I:J$, $\sqrt{I}$ 를 구해보자.

Theorem 5.

R : a commuative ring with 1, I is a ideal of R.

$1 \in I \quad \Rightarrow I=R$

proof :

$\forall r \in R, \quad r=r \cdot 1 \in I$

Definition 5.

$I+J=R$

I, J are relatively prime.

Note; 정수환에서 (2)+(3) $\ni$ $1=3-2$

$\therefore$ (2)+(3)=(1)=$\mathbb{Z}$ 가 된다는 생각을 확장한것.

Note.1.

$IJ \subset I \cap J$

$\because \ IJ \subset IR \subset I$

$IJ \subset RJ \subset J$

(4) Prime ideals (소 이데알)

$\mathbb{Z} \supset 3\mathbb{Z} \supset 6\mathbb{Z} \supset 12\mathbb{Z}$

$Z \supseteq 5Z \supseteq 10Z$

p가 소수 일 때, $p|ab \Rightarrow p|a$ or $p|b$ 이 성립한다.

$3\mathbb{Z} \supset 12\mathbb{Z} \Leftrightarrow 3|12$ 와 p : 소수의 성질을 다른 방법으로 표현해보자.

$ab \in p\mathbb{Z} \Rightarrow a \in p\mathbb{Z}$ or $b \in p\mathbb{Z}$

Definition 6.

R : a commutative ring with 1, P :a ideal of R

$ab \in P \Rightarrow a \in P$ or $b \in P$ 일 때, P is called a prime ideal

(5) Quotient rings

R is a comm. ring with 1, I : a ideal of R

$R/I = \{a+I \mid a \in R\}$: 당연히 group (R 가 Abel 군이므로)

합은 $(a+I)+(b+I) = (a+b)+I$

곱은 $(a+I)(b+I) = ab+I$ 로 정의 할수있을까?

(1) $a+I = a'+I \Leftrightarrow a-a' \in I$

$b+I = b'+I \Leftrightarrow b-b' \in I$ 일 때, $ab+I = a'b'+I$?

$ab-a'b' = a(b-b')+(a-a')b' \in I$ ← I가 ideal 이라면.

(2) $(a+i)(b+j) = ab+aj+bi+ij$, $i, j \in I$

$aj+bi \in I$ 이어야 한다. I : ideal 이라면.

이와같이 합과 곱이 잘 정의 된다면, R/I 은 환이된다.

이것을 quotient ring(상환) 이라한다.

Example 10.

① Z_n : ring

② $\mathbb{R}[x] \ni x^2+1$

x^2+1 : irreducible over $\mathbb{R}$

$< x^2+1 \geq (x^2+1)\mathbb{R}[x]$: ideal

$\Rightarrow \mathbb{R}[x]/< x^2+1 >$: quotient ring

$\ni f(x)+< x^2+1 > = q(x)(x^2+1)+(ax+b)+< x^2+1 >$

$= (ax+b)+< x^2+1 >$

한편 $r \in \mathbb{R}$, $r(ax+b+< x^2+1 >) = rax+rb+< x^2+1 >$와 같이

스칼라곱을 정의하면 $\mathbb{R}[x]/< x^2+1 >$ 은 R위의 vector space 이고

$\mathbb{R}[x]/< x^2+1 >$의 한 basis로 $\{1+< x^2+1 >, x+< x^2+1 >\}$ 를 갖는다.

한편,{1, I}는 C의 R위에서의 basis 이므로

$C \cong R[x]/< x^2+1 >$ 이다.

(6) Intergral domain, 정역

Definition 7.

D is a commutative ring with 1 without non trivial zero divisors

$\Rightarrow$ D is called an integral domain

Example 11.

① $\mathbb{Z}$: integral domain

② $\mathbb{Z}_5$: integral domain

③ $\mathbb{Z}_6$: not integral domain

$\because$ 2, 3 : zero divisors

Theorem 6.

p : prime $\Rightarrow$ $\mathbb{Z}_p$: integral domain

proof :

a, $b \in \mathbb{Z}_p$

let $ab = 0$ then $p \mid ab$

but p : prime, $p \mid a$ or $p \mid b$

hence $a = 0$ or $b = 0$ in $\mathbb{Z}_p$

Example 12.

$\mathbb{Z}_6[x] \ni x^2 - 3x + 2 = 0$

$x^2 - 3x + 2 = (x-1)(x-2) = 0$

$x = 1, 2, 4, 5$

Definition 8.

F : a commutative ring with 1

$\forall a \in F^* = F - \{0\}$ has a multiplication inverse 즉, $(F^*, \cdot)$: group

$\Rightarrow$ F : a field

Example 13.

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$

Theorem 7.

A finite integral domain is a field

proof :

Let $D = \{a_1, a_2, \cdots, a_n\}$ be an integral domain and all elements are distinct. 곱셈연산에 닫혀있으므로

$\forall a (\neq 0) \in D$, $aD = \{aa_1, \cdots, aa_n\} \subset D$ 이다.

But $aa_i = aa_j$ for some $i \neq j$

then $a(a_i - a_j) = 0$ in D

$\Rightarrow \quad a \neq 0, \quad a_i = a_j$ (모순)

Hence, aa_i : distinct $\forall i$

$\therefore \ |aD| = |D|$

$\therefore \ aD = D \ni 1$

$\therefore \ \exists a_R \in D \quad s.t. \quad aa_R = 1 \qquad a_R$: inverse of a

의문 : finite field는 $\mathbb{Z}_p$ 밖에 없는가?

F : finite field $\Leftrightarrow |F| = p^n, \quad p$: prime

(7) Ring Homomorphisms

$R, \ R'$: rings

$\varphi : R \rightarrow R'$ a map

such that ① $\varphi(a+b) = \varphi(a) + \varphi(b)$

② $\varphi(ab) = \varphi(a)\varphi(b)$

$\Rightarrow \ \phi$:a ring homomorphism from R to R'

Note; $\varphi(0) = 0'$

$\varphi(1) = 1'$

$\because \ \varphi(1) = \varphi(1 \cdot 1) = \varphi(1)\varphi(1)$ in R

R이 integral domain이면 cancellaion law가 성립함으로 $\varphi(1) = 1'$

또는, φ 가 onto 이면 $\exists a \in R$ s.t. $\varphi(a) = 1'$

$1' = \varphi(a) = \varphi(a \cdot 1) = \varphi(a)\varphi(1) = 1'\varphi(1) = \varphi(1)$

Example 14.

R :a commutative ring and $R \ni a$

$e_a : R[x] \rightarrow R, \ e_a(f(x)) = f(a)$ is an evaluation homomorphism.

$\because \ e_a(f(x) + g(x) = f(a) + g(a) = e_a(f(x)) + e_a(g(x))$

$e_a(f(x)g(x)) = f(a)g(a) = e_a(f(x))e_a(g(x))$

Basic properties of a ring homomorphism.

$\varphi : R \rightarrow R'$ is a ring homomorphism

Then,

① $\varphi(0) = 0'$

② $\varphi(-a) = -\varphi(a)$

③ $\varphi(a^n) = \varphi(a)^n$

$\because \ \varphi(a^n) = \varphi(a \cdots a) = \varphi(a) \cdots \varphi(a) = \varphi(a)^n$

④ a : unit

$\Rightarrow \ \varphi(a)$: unit of R'

$\because \ a$: unit $\Rightarrow \exists b \in R \ \ s.t. \ \ ab = 1$

$$\varphi(a)\varphi(b)=\varphi(ab)=\varphi(1)=1'$$
$$\therefore\ \varphi(a)\ :\ \text{unit in}\quad R'$$

⑤ $\varphi(a^{-n})=\varphi(a)^{-n}$

$$\because\ \varphi(a^{-n})\varphi(a)^n=\varphi(a^{-1}a^{-1}\cdots a^{-1})\varphi(a)\varphi(a)\cdots\varphi(a)$$
$$=1\ '$$
$$\therefore\ \varphi(a)^{-n}=\varphi(a^{-n})$$

⑥ S : subring of $R\ \Rightarrow \varphi(S)$: subring of R'

$$\because\ \varphi(a),\ \varphi(b)\in\varphi(S),\ \varphi(a)-\varphi(b)=\varphi(a-b)\in\varphi(S)$$
$$\varphi(a)\varphi(b)=\varphi(ab)\in\varphi(S)$$

⑦ S' : subring of $R'\ \Rightarrow \varphi^{-1}(S')$: subring of R

$$\because\ a,\ b\in\varphi^{-1}(S'),\ \varphi(a-b)=\varphi(a)-\varphi(b)\in S'$$
$$\varphi(ab)=\varphi(a)\varphi(b)\in S'$$
$$\therefore\ a-b\in\varphi^{-1}(S'),\ ab\in\varphi^{-1}(S')$$

⑧ I : ideal of $R\ \Rightarrow \varphi(I)$: ideal of $\varphi(R)$

$$\because\ \varphi(a)\in\varphi(I),\ \varphi(r)\in\varphi(R)$$
$$\varphi(a)\varphi(r)=\varphi(ar)\in\varphi(I)\ \ (\ I:\ \text{ideal of}\quad R)$$

R'의 원소를 φ로 표현하기 위해서는 공변역을 $\varphi(R)$로 보면 가능함.

⑨ I' : ideal of $R'\ \Rightarrow \varphi^{-1}(I')$: ideal of R

$$\because\ \forall a,\ b\in\varphi^{-1}(I')\ \Rightarrow a-b\in\varphi^{-1}(I')\ ?$$
$$\varphi(a-b)=\varphi(a)-\varphi(b)\in I'$$
$$\forall a\in\varphi^{-1}(I'),\ r\in R\ \Rightarrow ar\in\varphi^{-1}(I')\ ?$$
$$\varphi(ar)=\varphi(a)\varphi(r)\in I'$$

Theorem 8. Fundamental Theorem of Rings

$\varphi: R\to R'$:a ring homomorphism, $\ker\varphi=I$

$$\Rightarrow\ \exists\,\varphi^*: R/I\to\varphi(R)\ \ s.t.\ \ \varphi^*\ :\ \text{a ring isomorphism}$$

Proof;

① $\varphi^*(a+I)=\varphi(a)$: well-defined ?

$a+I=b+I\ \Rightarrow\ \phi(a)=\phi(b)$?

$a-b\in I=\ker\varphi$

$\varphi(a-b)=0\qquad\therefore\ \varphi(a)-\varphi(b)=0$

② homomorphism.?

$$\varphi^*((a+I)+(b+I))=\varphi^*((a+b)+I)=\varphi(a+b)$$
$$=\varphi(a)+\varphi(b)=\varphi^*(a+I)+\varphi^*(b+I)$$
$$\varphi^*((a+I)(b+I))=\varphi^*(ab+I)=\varphi(ab)$$
$$=\varphi(a)\varphi(b)=\varphi^*(a+I)\varphi^*(b+I)$$

③ 1-1?

$$\ker\varphi^*=\{a+I\in R/I\mid\varphi^*(a+I)=0\}$$

$$a+I\in\ker\varphi^*,\quad \varphi^*(a+I)=\varphi(a)=0$$
$$\therefore\ a\in\ker\varphi=I$$
$$\therefore\ \ker\varphi^*=\{I\}$$

Therefore

$R/\ker\varphi\cong\varphi(R)=Im\varphi$

Example 15.

$\varphi:\ \mathbb{C}\to\left\{\begin{pmatrix} a & b\\ -b & a\end{pmatrix}\,\middle|\, a,\ b\in\mathbb{R}\right\},\ \varphi(a+bi)=\begin{pmatrix} a & b\\ -b & a\end{pmatrix}$

Then ① φ : homomorphism

② φ : 1-1

③ φ : onto

Example 16.

$\mathbb{Q}[x]\ni x^2-2=p(x)$: irreducible in $\mathbb{Q}[x]$

$p(\sqrt{2})=0$ in $\mathbb{R}$ 이므로 evaluation map $e_{\sqrt{2}}$를 정의한다.

Define $e_{\sqrt{2}}:\ \mathbb{Q}[x]\to\mathbb{R},\ e_{\sqrt{2}}(f(x))=f(\sqrt{2})$

Then $e_{\sqrt{2}}$: homomorphism.

$$\ker e_{\sqrt{2}}\ =\ \{f(x)\in\mathbb{Q}[x]\mid f(\sqrt{2})=0\}\subset\mathbb{Q}[x]$$

$\mathbb{Q}[x]$: P.I.D. (integral domain이면서 모든 ideal이 하나로 생성된다.)

그런데, $\ker e_{\sqrt{2}}$는 $\mathbb{Q}[x]$의 ideal이므로,

$\ker e_{\sqrt{2}}$는 하나의 원소로 생성된다.

즉, $<x^2-2>\ \supseteq\ \{f(x)\in\mathbb{Q}[x]\mid f(\sqrt{2})=0\}$

$\mathbb{Q}[x]/<x^2-2>\cong Im e_{\sqrt{2}}=e_{\sqrt{2}}(\mathbb{Q}[x])$

$$=\mathbb{Q}[\sqrt{2}]=\{a+b\sqrt{2}\mid a,\ b\in\mathbb{Q}\}\ :\ \text{field}$$

(8) Polynomials(다항식환)

Definition 8.

① R : a commutative ring with 1

$R[x]=\{a_0+a_1x+\cdots+a_nx^n\mid a_i\in R\}$: a commutative ring with 1

$R((x))=\left\{\sum^{\infty}a_ix^i\,\middle|\, a_i\in R\right\}$: power series ring

$$\because\ (\sum a_ix^i)(\sum b_jx^j)=\sum c_kx^k,\quad c_k=\sum_{i+j=k}a_ib_j$$

$R[x]\subset R((x))$ subring 이되고, $R[x]$를 다항식환이라 한다.

② D : integral domain $\Rightarrow D[x]$: integral domain

③ F : field $\Rightarrow F[x]$: field ?

반례 : $\mathbb{R}[x] \ni 1-x$

$\frac{1}{1-x} = 1 + x + \cdots + x^n + \cdots \notin \mathbb{R}[x]$

(9) Field of quotients

D :an integral domain, $D^* = D - \{0\}$

$D \times D^* = \{(a,b) \mid a,\ b \in D,\ b \neq 0\}$

$(a,b) \sim (c,d) \iff ad = bc$

then $\sim$ is an equivalence relation

$\because$ transitive ?

$ad = bc,\ cf = de \Rightarrow af = be$?

$adf = bcf \quad adf = bde \quad \therefore\ af = be$

Hence $D \times D^* / \sim = \{[(a,b)]\}$: field ?

Define $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd},\ \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$

① well-defined?

② $\frac{a}{b} \neq 0$ ($a \neq 0$이다. $a = 0$이면 $\frac{a}{b} = 0$이니까)

따라서 $\exists \frac{b}{a}$ s.t. $\frac{a}{b}\frac{b}{a} = 1$

만약 $D = \mathbb{Z}$ 라면 $\mathbb{Z} \times \mathbb{Z}^* / \sim \equiv \Phi(\mathbb{Z}) \cong \mathbb{Q}$

$D = F[x]$ 라면 $\Phi(F[x]) = F(x)$:field of the rational functions

<연습문제>

1. Suppose that R is a ring and that $a^2 = a$ for all a in R. Show that R is commutative.

2. Let F be a field of order 3^n. Prove that $\mathrm{char} F = 3$.

3. Show that $A = \{(3x,\ y) \mid x,\ y \in Z\}$ is a maximal ideal of $Z \oplus Z$.

4. Let A, B and C be subrings of a ring R. If $A \subseteq B \cup C$, show that $A \subseteq B$ or $A \subseteq C$.

5. Determine all ring homomorphism from Z_6 to Z_6

Determine all ring homomorphism from Z_{20} to Z_{30}

6. Let $R=\left\{\begin{pmatrix} a & b \\ b & a \end{pmatrix} \mid a, b \in Z\right\}$. Let ϕ be the mapping that takes $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$ to $a-b$.

ⓐ Show that ϕ is a homomorphism

ⓑ Is $\ker\phi$ a prime ideal or maximal ideal?

7. Let $f(x)=5x^4+3x^3+1$ and $g(x)=3x^2+2x+1$ in $Z_7[x]$.
Determine the quotient and remainder upon dividing $f(x)$ by $g(x)$.

8. Let F be a field and let $I=\{f(x)\in F[x] \mid f(a)=0 \text{ for } all\ a \in F\}$
Prove that I is an ideal in $F[x]$.
Prove that I is infinite when F is finite and $I=\{o\}$ when F is infinite.

9. Prove that the ideal $<x^2+1>$ is prime in $Z[x]$.
but not maximal in $Z[x]$.

10. Show that $Z[\sqrt{-6}]$is not a unique factorization domain.
why does this show that $Z[\sqrt{-6}]$is not a principal ideal domain?

11. If R is a commutative ring and I and J are two proper ideal with $I+J=R$, prove that $R/(I\cap J)$ is isomorphic to $R/I \oplus R/J$.

12. Suppose that R is a commutative ring and I is an ideal of R. prove that $R[x]/I[x]$ is isomorphic to $(R/I)[x]$.

13. If $)R[x]$ is an principal ideal domain then R must be a field.

3. Fields, 체

체(Field)의 정의

A field F is a commutative ring with $1 \neq 0$ in which every nonzero element a is a unit: that is $a^{-1} \in F$ with $a^{-1}a = 1$.

(1) Basic properties of fields

Theorem 1.

F is a field, I a non zero ideal of F $\Rightarrow$ $I = F$

proof :

$\exists\, a \neq 0 \in I \subset F$ s.t. $ab = 1 \in I$

$\forall\, x \in F$, $x = x \cdot 1 \in I$

Theorem 2.

F_1, F_2 : fields, $\varphi : F_1 \rightarrow F_2$:a ring homomorphism and $\varphi \neq 0$

$\Rightarrow \varphi$: 1-1

proof :

$\ker\varphi$: ideal of F_1

since $\varphi \neq 0$, $\ker\varphi = \{0\}$

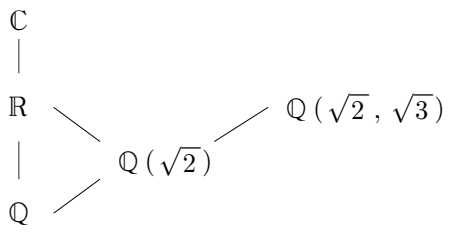
therefore $\phi : F_1 \rightarrow \phi(F_1) \subset F_2$

$F_1 \cong \varphi(F_1) \subset F_2$ subfield

Example 1.

field들 사이에 환의 연산이 보존되면 subfield 관계를 갖는다.

$\mathbb{Z}_3 \not\subset \mathbb{Z}_5$



Theorem 3.

F is a subfield of K (K is an extension field of F)

$\Rightarrow$ K is a vector space over F

proof :

since $F \leq K$

$\cdot : F \times K \to K$: scalar procuct $\cdot(a, \alpha) = a \cdot \alpha$ the multiplication in K

$\dim_F K = [K : F] = n < \infty$

Therefore K is a finite extension of F

Example 2.

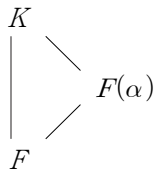
$\mathbb{Q}[\sqrt{2}] \ni a + b\sqrt{2}$

$|$ $\quad\therefore\quad \{1, \sqrt{2}\}$ is a basis of $\mathbb{Q}(\sqrt{2})$

$\mathbb{Q}$ $\quad\quad [\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$

Definition 1.

$F(\alpha)$ is the samllest subfield of K containing α and F



$A = \bigcap_{i \in \Gamma} K_i,\ F \subset K_i \leq K$ subfield, $\alpha \in K_i$

$B = \left\{ \dfrac{f(\alpha)}{g(\alpha)} \,\middle|\, f(x),\ g(x) \in F[x],\ g(\alpha) \neq 0 \right\}$

$A = B$?

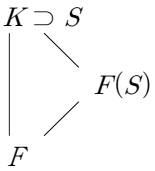
$\alpha = \dfrac{\alpha}{1} \in B, \quad a \in F, \quad a \in B \qquad \therefore\ F \subset B$

B : field $\qquad\qquad \Rightarrow A \subset B$

$\forall \dfrac{f(\alpha)}{g(\alpha)} \in B,\ \dfrac{f(\alpha)}{g(\alpha)} = \dfrac{b_0 + b_1\alpha + \cdots + b_m\alpha^m}{a_0 + a_1\alpha + \cdots + a_n\alpha^n} \in K_i, \quad \forall i$

$\therefore\ \forall i,\ B \subset K_i,\ B \subset \bigcap K_i = A$

$F(S)$ = the smallest subfield of K containing S and F



즉, $\left\{ \dfrac{f(\alpha_1, \cdots, \alpha_v)}{g(\beta_1, \cdots, \beta_u)} \,\middle|\, \alpha_1, \cdots, \alpha_v, \beta_1, \cdots, \beta_u \in S,\ g(\beta_1, \cdots, \beta_u) \neq 0 \right\}$

$$f(x_1, \cdots, x_v) = \sum a_{r_1 \cdots r_v} x_1^{r_1} \cdots x_v^{r_v}$$

두 변수의 예를 들면,

$$f(x, y) = a_{00} + a_{10}x + a_{01}y + a_{11}x^1y^1 + \cdots + a_{ij}x^iy^j + \cdots$$
$$= \sum a_{ij}x^iy^j$$

여기서 $F(\alpha) \ni \dfrac{f(\alpha)}{g(\alpha)}$의 유리식 표현에서 분모인 $\dfrac{1}{g(\alpha)}$를 polynomial 로 표현할 수 있을까?

(2) 초월수와 대수적인 수

Definition 2.

① $F \le K$, $\alpha \in K$, α is an algebraic over F

$\Leftrightarrow \exists f(x) \in F[x]$ $s.t.$ $f(\alpha) = 0$

② $F \le K$, $\alpha \in K$, α is not algebraic over F then α is a transcendental over F

③ $F \le K$, $\forall \alpha \in K$, α : algebraic over F

$\Rightarrow$ K : algebraic extension of F

ex. $\mathbb{Q}(\sqrt{2})$ | $\mathbb{Q}$ $\mathbb{C} = \mathbb{R}[i]$ | $\mathbb{R}$

Theorem 4. 크로네커 정리

$f(x) \in F[x]$, $\deg(f) > 0$

$\Rightarrow$ $\exists K \ge F$, $\alpha \in K$ $s.t.$ $f(\alpha) = 0$

이런 K와 α를 구성하기 위해서는 환의 이론을 좀 더 살펴보자.

Definition 3. Maximal ideals

R : a comm. ring with 1

M : a maximal ideal of R

$\Leftrightarrow$ N : ideal of R s.t. $M \subset N \subset R$

then $N = M$ or $N = R$

Theorem 5.

R is a commutative ring with 1, M is a ideal of R

M : maximal ideal of R $\Leftrightarrow$ R/M : field

proof :

$\varphi : R \to R/M$, $\varphi(r) = r + M$: ring homo.

$\ker\varphi = \{M\}$

R ←--φ--→ R/M

| |

M ←-----→ (0)

R 와 R/M 의 ideal 들 사이에 1-1 대응이 성립함을 보이자.

Theorem 6.

Let $\varphi : R \to R'$ is a ring homomorphism and onto. and $Ker\phi = K$

$X = \{I \mid K \subset I : ideal\ of\ R\}$

$Y = \{I' \mid I' : ideal\ of\ R'\}$ 이면

$X \approx Y$

Proof of step 1.

Define $f: X \to Y,\ f(I) = \varphi(I)$: ideal of R' ($\because$ φ is onto)

$g: Y \to X,\ g(I') = \varphi^{-1}(I)$: ideal of R

then $K \subset \varphi^{-1}(I)$

$\because\ \varphi^{-1}(0) = K$ 이고 $0 \subset I$ 이므로

$K \subset \varphi^{-1}(I)$

Therefore $(g \circ f)(I) = \varphi^{-1}(\varphi(I)) = I$?

$(f \circ g)(I') = \varphi(\varphi^{-1}(I')) = I'$?

일반적으로 $\varphi^{-1}(\varphi(I)) \supset I$

$\varphi^{-1}(\varphi(I)) \subset I$?

$b \in \varphi^{-1}(\varphi(I)) \Rightarrow \varphi(b) \in \phi(I) \Rightarrow \varphi(b) = \varphi(c)$ for some $c \in I$

$\Rightarrow \varphi(b) - \varphi(c) = 0 \Rightarrow b - c \in \ker\varphi = K \subset I$

$\Rightarrow\ b - c = i \quad \therefore\ b = c + i \in I$

일반적으로 $\varphi(\varphi^{-1}(I')) \subset I'$

$\varphi(\varphi^{-1}(I')) \supset I'$?

$\forall\, b \in I' \supset R'$, since ϕ is onto, $\exists\, b \in R$ s.t. $\varphi(b) = b' \in I'$

$\therefore\ b \in \varphi^{-1}(I'),\ b' = \varphi(b) \in \varphi(\varphi^{-1}(I'))$

(3) Finite extension and Algebraic extension(유한확대와 대수적확대)

Theorem 6.

If K is a finite extension of F then it is an algebraic extension

proof :

K $\quad$ $[K:F] = n < \infty$

$|$ $\quad$ $\forall\, \alpha (\neq 0) \in K$, α is algebraic over F ?

F

Consider the elements

$\{1,\ \alpha,\ \alpha^2, \cdots,\ \alpha^n\} \subset K$

$\{1,\ \alpha,\ \alpha^2, \cdots,\ \alpha^n\}$: linearly dependent over F.

Therefore $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$ for some $a_0, \cdots, a_n$

which is not all zeros in F.

Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in F[x]$

then $f(\alpha) = 0$

Hence α is algebraic over F

Theorem 7.

$F \leq K,\ \alpha \in K$

$\overline{F_K} = \{\alpha \in K \mid \alpha$: algebraic over $F\}$ is the algebraic closure of F in K

$\Rightarrow \overline{F_K}$: subfield of K

proof :

$\forall \alpha, \beta \in \overline{F_K}$

$F(\alpha, \beta) = (F(\alpha))(\beta)$: finite extension of F

lemma 8.
$$\begin{array}{l} L \\ | \\ K \\ | \\ F \end{array} \qquad \begin{array}{l} [L:K] = m,\ [K:F] = n \\ \Rightarrow [L:F] = nm \end{array}$$

proof :

Let $\{\alpha_1, \cdots, \alpha_n\}$ be a basis for K over F

$\{\beta_1, \cdots, \beta_m\}$ be a basis for L over K

then $\{\alpha_i \beta_j\} \subset L$

Claim : $\{\alpha_i \beta_j\}$: basis for L over F

$\forall r \in L,\ r = a_1\beta_1 + \cdots + a_m\beta_m,\ a_i \in K$

but $a_i \in K,\ a_i = \sum_{j=1}^{n} a_{ij}\alpha_j$

hence $r = \sum a_i\beta_i = \sum_{i=1}^{m} (\sum a_{ij}\alpha_j)\beta_i = \sum_{i,j} a_{ij}\alpha_j\beta_i$

lemma 9.
$$\begin{array}{l} K \ni \alpha \\ | \\ F(\alpha) \\ | \\ F \end{array} \qquad [F(\alpha):F] \ = ?$$

proof :

$e_\alpha : F[x] \to K,\ e_\alpha(f(x)) = f(\alpha)$: homo.

$F[x]/\ker e_\alpha \cong Im e_\alpha = F[\alpha] \leq K$

$\ker e_\alpha = < p(x) >$, where $p(\alpha) = 0$, $\deg p(x)$: minimal deg.

$\nwarrow F[x]$: P.I.D.

이때 $p(x)$: 기약 in $F[x]$

$\because\ p(x) = p_1(x)p_2(x)$라 하면, $p(\alpha) = p_1(\alpha)p_2(\alpha) = 0$

$p_1(\alpha) = 0$ or $p_2(\alpha) = 0$ ($F[x]$: integral domain) ... 모순

$\deg p(x) = [F(\alpha):F]$

Example 3.

$$\begin{array}{l} \mathbb{C} \ni i \\ | \\ \mathbb{R} \end{array}$$: algebraic over $\mathbb{R}$

$p(x) = x^2 + 1, \quad \mathbb{R}[x]/ < x^2 + 1 > \cong \mathbb{R}[i]$

lemma 10. $F[x] \ni p(x)$

$p(x)$ is a irreducible polynomial $\Leftrightarrow < p(x) >$ is a maximal ideal of $F[x]$

proof :

($\Rightarrow$) consider $< p(x) > \subset N \subset F[x]$ $s.t.$ N : ideal of $F[x]$

since $F[x]$: P.I.D.

$N = < f(x) >$ for some $f(x) \in F[x]$

therefore $< p(x) > \subset < f(x) > \subset F[x]$

$p(x) \in < f(x) >$, $p(x) = f(x)q(x)$ for some $q(x) \in F[x]$

But, $p(x)$ is irreducible over F,

either $f(x)$ is constant or $q(x)$ is contant

(1) $f(x)$ is constant $\Rightarrow < f(x) \geqq F[x]$

(2) $q(x)$ is constant $\Rightarrow < f(x) \geqq < p(x) >$

($\Leftarrow$) $p(x) = p_1(x)p_2(x)$, $\quad \deg p > \deg p_1$, $\deg p_2$

then $< p(x) > \ni p(x) = p_1(x)p_2(x)$

since $< p(x) >$ is a prime ideal,

$< p(x) > \ni p_1(x)$ or $< p(x) > \ni p_2(x)$

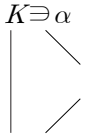
hence $p_1(x) = p(x)q(x) = p_1(x)p_2(x)q(x)$

$\Rightarrow 1 = p_2(x)q(x)$

$\deg 1 = 0$, $\deg p_2(x)q(x) = n > 0$ ... 모순

Therefore $\mathbb{R}[x]/ < x^2 + 1 > \cong \mathbb{R}[i]$ is field

$\mathbb{R}(i)$: 분수식이면서 i와 $\mathbb{R}$을 품는 제일 작은 field



α : algebraic

$F[x]/ < p(x) > \cong F[\alpha] = F(\alpha)$

field! | ?

F

Theorem 11.

$K \supseteq \alpha$ is an algebraic over F

$|$

F

$p(x)$ is the irreducible monic polynomial of α over F with $\deg p(x) = n$

$\Rightarrow [F[\alpha] : F] = n$

proof :

$F[\alpha] \cong F[x]/ < p(x) >$

Let $p(x) = x^n + a_1 x^{n-1} + \cdots + a_n$, $\quad a_n \neq 0$

then $p(\alpha) = \alpha^n + a_1 \alpha^{n-1} + \cdots + a_n = 0$

$\therefore \alpha^n = -a_1 \alpha^{n-1} - \cdots - a_n$

$\{1,\ \alpha,\ \alpha^2, \cdots,\ \alpha^{n-1}\}$ are linearly independent in $F[\alpha]$

$\because\ b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} = 0$ for some not all zero

$$g(x) = b_0 + b_1 x + \cdots + b_{n-1}x^{n-1} \in F[x]$$

$g(x) = 0,\ \deg g(x) = n-1$ ...모순

주제로 돌아와서

$K \supset \alpha,\ \beta$: algebraic over F

$F(\alpha, \beta)$

F ↖ finite extention ?

$\overline{F_K} \supset \alpha,\ \beta,$ $F(\alpha, \beta)$ is an: algebraic extension

$\supset\ \alpha+\beta,\ \alpha\beta,\ \alpha/\beta\ (\beta \neq 0)$: algebraic over F

therefore $F(\alpha, \beta) \subset \overline{F_K}$

Definition 4.

$\mathbb{C}$

|

$\mathbb{Q}$

$\overline{\mathbb{Q}_{\mathbb{C}}}$: the set of all algebraic elements in $\mathbb{C}$ over $\mathbb{Q}$

is called the algebraic numbers (대수적인 수)

$\mathbb{C} - \overline{\mathbb{Q}_{\mathbb{C}}}$ is called the transcendentals(초월수)

(4) The characteristic of a ring

R : a ring

$m = \min\{n > 0 \mid a + a + \cdots + a = na = 0, \forall\, a \in R\} \subset \mathbb{N}$

: is called the characteristic of R , $ch(R)$

Example 4.

$Ch(\mathbb{Z}_4) = 4$

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

Theorem 12.

R is a commutative ring with 1

$$\Rightarrow\ Ch(R) = \min\{n \mid 1 + \cdots + 1 = n \cdot 1 = 0\}$$

$\because\quad \forall\, a \in R,\ a = a \cdot 1$

$$a + \cdots + a = a \cdot 1 + \cdots + a \cdot 1 = a(1 + \cdots + 1)$$

Example 5.

$Ch(\mathbb{Z}) = 0$

$Ch(\mathbb{Q}) = 0$ 이다.

Theorem 13.

D is a integral domain with 1

Then $Ch(D)=0$ or $Ch(D)=p$: prime

proof :

$Ch(D)\neq 0$ then $Ch(D)=n$

if $n=n_1n_{2,},\ n_1<n,\ n_2<n$

then $0=n\cdot 1=(n_1n_2)\cdot 1=1+\cdots+1$

$=(1+\cdots+1)(1+\cdots+1)=(n_1\cdot 1)(n_2\cdot 1)=0$

$\Rightarrow n_1\cdot 0=0$ or $n_2\cdot 1=0$ ... 모순

Theorem 14.

R is aa commutative ring with 1

$\Rightarrow \exists\varphi:\ \mathbb{Z}\to\mathbb{R},\ \varphi(n)=1+\cdots+1=n\cdot 1,$ when $n>0$

$\varphi(n)=(-1)+\cdots+(-1)=(-n)\cdot(-1),$ when $n<0$

$\varphi(0)=0$: ring homomorphism.

proof : ($n>0$, $m<0$ 일 때는 별도로 계산해 보면 된다.)

$\varphi(n+m)=(n+m)\cdot 1=1+\cdots+1=(1+\cdots+1)+(1+\cdots+1)$

$n\cdot 1+m\cdot 1=\varphi(n)+\varphi(m)$

$\varphi(nm)=(-nm)(-1)=(1+\cdots+1)((-1)+\cdots+(-1))=\varphi(n)\varphi(m)$

Theorem 15.

K : a field

$\Rightarrow\ \exists\phi:\ \mathbb{Z}\to K$ is a ring homomorphism.

If (1) $\ker\varphi=\{n\in\mathbb{Z}\mid n\cdot 1=0\}\neq 0$

then $\ker\varphi=p\mathbb{Z}$

$\mathbb{Z}/p\mathbb{Z}\cong Im\varphi\leq K$

$=\mathbb{Z}_p$

(2) $\ker\varphi=0\ \Leftrightarrow Ch(K)=0$

then $\mathbb{Z}\cong Im\varphi\leq K$

Theorem 16.

D is a integral domain

$\Phi(D)$ is the quotient field of D

F a field such that $D\subset F\ \Rightarrow \Phi(D)\leq F$

proof :

① $f:D\to\Phi(D),\ f(a)=\dfrac{a}{1}$: 1-1, homomorphism.

$f(a+b)=\dfrac{a+b}{1}=\dfrac{a}{1}+\dfrac{b}{1}=f(a)+f(b)$

$f(ab)=f(a)f(b)$

$$\ker f = \left\{ a \in D \mid \frac{a}{1} = 0 \right\} = (0)$$

② $\varphi(D) \to F$ 로 1-1, homomorphism인 함수를 만들면 된다.

$\phi(a, b) = ab^{-1}$

(1) ϕ : well defined ?

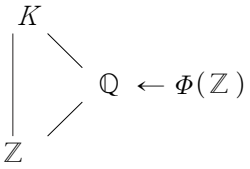
즉, $\frac{a}{b} = \frac{c}{d} \Rightarrow ab^{-1} = cd^{-1}$?

$a, b, c, d \in D \subset F$

$\Rightarrow ad = bc, \ a = bcd^{-1} \qquad \therefore \ ab^{-1} = cd^{-1}$

(2) homomorphism.

Hence K s.t. $Ch(K) = 0$, K : field



Theorem 17.

F is a field, $|F| = p$

K is a finite extension of F

$[K:F] = n$

$\Rightarrow |K| = p^n$

proof :

$[K:F] = n \Rightarrow K \supset \{\alpha_1, \cdots, \alpha_n\}$ is a basis of K over F

$\forall \alpha \in K, \ \alpha = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n, \quad a_i \in F$

Since the expression is unique

$\therefore |K| = p^n$

(5) 크로네커 정리

Theorem 18. Kronecker's 정리

$F[x] \ni f(x)$

$\Rightarrow \exists E$ is an extension field of F and $\alpha \in E$ s.t. $f(\alpha) = 0$

proof :

Since $F[x]$ is UFD, $f(x) = p(x)f_1(x)$, $p(x)$: irreducible.

$E = F[x] / < p(x) >$ is field

Take $\alpha = x + < p(x) > \in E$

$f(x) = p(\alpha)f_1(\alpha)$, $p(\alpha) = 0$ in E

$p(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x], \quad a_n \neq 0$

but $F \hookrightarrow F[x] \to F[x]/ < p(x) >$
$a \to a \to a + < p(x) >$

$\phi \neq 0$, ϕ : 1-1

$\therefore$ $F \leq E$

claim 1 $p(\alpha) = (a_0 + < p(x) >) + (a_1 + < p(x) >)(x + < p(x) >)$
$+ \cdots + (a_n + < p(x) >)(x + < p(x) >)^n$ in E

$\therefore$ $p(\alpha) = (a_0 + < p(x) > + \cdots + (a_n + < p(x) >)(x^n + < p(x) >)$
$= (a_0 + a_1 x + \cdots + a_n x^n) + < p(x) >$
$= 0$ in E

Example 5.

원소의 갯수가 4개인 field를 구성해보자.

$\mathbb{Z}_2(\alpha)$ a basis for $\mathbb{Z}_2(\alpha)$ over $\mathbb{Z}_2$
|
$\mathbb{Z}_2$

2차인 기약의 polynomial를 만들자.

$\mathbb{Z}_2[x] \ni p(x) = x^2 + x + 1$: 기약

$\exists K$: field s.t. $\mathbb{Z}_2 \leq K$ and $p(\alpha) = 0$, $\alpha \in E$

$K = \mathbb{Z}_2[x]/ < x^2 + x + 1 >$, $\alpha = x + < x^2 + x + 1 >$

그런데 $K = \mathbb{Z}_2(\alpha)$이므로, $\mathbb{Z}_2 = \{0, 1, \alpha, 1+\alpha\}$

$\cdot$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

→ 곱셈에 대한 group

원소의 개수가 8개인 field의 구성

$\mathbb{Z}_2(\alpha) \ni \{1, \alpha, \alpha^2\}$
|
$\mathbb{Z}_2$

$\alpha^3 + \alpha + 1 = 0$

$x^3 + x + 1 = p(x) \in \mathbb{Z}_2[x]$

$GF(2^3) \equiv \mathbb{Z}_2(\alpha) = \{0, 1, \alpha, \alpha^2, 1+\alpha, 1+\alpha^2, \alpha+\alpha^2, 1+\alpha+\alpha^2\}$

(6) Insolvability of The General Quintic

$f(x) \in k[x] \subset K_1[x] \subset K_2[x] \cdots$

by Kronecker's 정리

$\exists z_1 \in K_1$ s.t. $f(z_1) = 0$, $f(x) = (x - z_1) f_1(x)$, $f_1(x) \in K_1[x]$
$z_2 \in K_2$ s.t. $f_1(z_2) = 0$, $\cdots$
$\cdots$

$z_1,\ z_2, \cdots,\ z_n \in E$: extension field of k

In $E[x]$,

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$
$$= (x - z_1)(x - z_2) \cdots (x - z_n)$$
$$a_{n-1} = -(z_1 + \cdots + z_n)$$
$$a_{n-2} = \sum_{i<j} z_i z_j$$
$$\cdots$$
$$a_0 = (-1)^n z_1 \cdots z_n$$

The smallest extension field of k containing all zero of $f(x)$

$\equiv$ the splitting field of $f(x)$ of k

$= k(z_1,\ z_2, \cdots,\ z_n)$, where $z_1, \cdots, z_n$ are zeros of $f(x)$

Theorem 19.

$$\begin{array}{c} K \\ | \\ F \end{array}$$

$G(K/F) = \{\sigma \mid \sigma :\ K \to K$: automorphism, $\sigma(a) = a,\ \forall\, a \in F\}$

$\Rightarrow\ G(K/F)$ is a subgroup of the symmetric group S

proof :

$\forall\, \sigma,\ \tau \in G(K/F),\quad \sigma \circ \tau \in G(K/F),\ \sigma^{-1} \in G(K/F)$

Let E be a splitting field of k,

$G(E/k)$: the Galois group of E over k

Example 6.

$\mathbb{Q}[x] \supset x^2 - 2 = f(x)$

$G(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{1,\ \varphi_{\sqrt{2},-\sqrt{2}}\}$

$$\mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$$
$$\sqrt{2} \ \to\ \sqrt{2}$$
$$\sqrt{2} \ \to\ -\sqrt{2}$$

$f(x) = ax^2 + bx + c \in \mathbb{Q}[x]$

$\Rightarrow\ \exists\, \alpha \in K$ s.t. $f(\alpha) = 0$

$$\begin{array}{c} | \\ \mathbb{Q} \end{array}$$

$x = \dfrac{-b \pm \sqrt{D}}{2a}$ 이므로, $\mathbb{Q} \le K = \mathbb{Q}(\sqrt{D})$

방정식을 푼다는 것은 field 에서 보면 radical field의 chain이 존재하여 그 안에 splitting field가 품긴다는 의미이다.

Normal extension 관계 (예: $\mathbb{Q}$상의 extension처럼) 이면

K

$[K:F] = |G(K/F)| = \{K:F\}$

F

K 와 F 사이의 모든 field 는 $G(K/F)$의 부분군들과 서로 1-1 대응관계를 갖고 있다.

Theorem 20.

$k \le K$

$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in k[x]$

$E = k(z_1, z_2, \cdots, z_n)$ is the splitting field of $f(x)$ over k

$\sigma : E \to E$ is an automorphism

$\Rightarrow$ ① $\sigma(a) = a, \ \forall a \in k$ (즉, $\sigma \in G(E/k)$)

then $\sigma|_Z : Z \to Z$ bijection, $Z = \{z_1, z_2, \cdots, z_n\}$

② $\sigma : Z \to Z$ bijection

then $\sigma(a_i) = a_i, \ i = 0, 1, 2, \cdots, n-1$

proof :

① $z_1 \in Z, \ \sigma(z_1) \in Z$?

z_1 : root of $f(x)$ $\Rightarrow 0 = f(z_1) = z_1^n + a_{n-1}z_1^{n-1} + \cdots + a_1 z_1 + a_0$ in E

$f(\sigma(z_1)) = \sigma(z_1)^n + a_{n-1}\sigma(z_1)^{n-1} + \cdots + a_1\sigma(z_1) + a_0$

$= \sigma(z_1^n + a_{n-1}z_1^{n-1} + \cdots + a_1 z_1 + z a_0) = \sigma(f(z_1)) = \sigma(0) = 0$

$\therefore \ \sigma|_Z : Z \to Z$ map

$\sigma|_Z$: 1-1. ($\because$ σ : 1-1)

since Z : finite, $\sigma|_Z$: onto

② $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = (x - z_1)(x - z_2)\cdots(x - z_n)$

$a_{n-1} = -(z_1 + \cdots + z_n)$

$\sigma(a_{n-1}) = \sigma(-(z_1 + \cdots + z_n))$

$= -\sigma(z_1 + \cdots + z_n)$

$= -(\sigma(z_1) + \cdots + \sigma(z_n))$ $\because$ σ : onto

$= -(z_1 + \cdots + z_n)$ $\because$ σ : permutation

$= a_{n-1}$

Lemma.21.

$E = k(z_1, \cdots, z_n)$

$\sigma : E \to E$ onto, fixed k 즉, $\sigma \in G(E/k)$

$\sigma(z_i) = z_i, \quad \forall i$

$\Rightarrow \sigma : E \to E$ identity

proof :

By induction on n,

i) $n = 1, \ E = k(Z) \ni \dfrac{f(z)}{g(z)}, \ f(z), \ g(z) \in k[z]$

$\sigma(f(z))=f(z),\ \sigma(g(z))=g(z)$

$\sigma(\frac{f(z)}{g(z)})=\frac{f(z)}{g(z)}$

$E=K(Z_n)$
|
$K=k(z_1,\cdots,\ z_{n-1})$
|
k

ii) $n-1$ 일 때 성립을 가정하면,

$K=k(z_1,\cdots,\ z_{n-1})$ 일 때, $E=K(Z_n)$ 이므로 clear.

Theorem 22.

$f(x)\in k[x],\ \deg f=n$

E : splitting field of $f(x)$ over k

$\Rightarrow$ $G(E/k)$ is isomorphism to a subgroup of symmetric group S_n

proof :

Define $\varphi:\ G(E/k)\to S_n,\ \varphi(\sigma)=\sigma|_X,\ X=\{z_1,\cdots,\ z_n\}$

- φ : map
- $\varphi(\sigma\tau)=\sigma\circ\tau|_X=\sigma|_X\circ\tau|_X=\varphi(\sigma)\varphi(\tau)$

  $\forall\, z\in X,\ (\sigma\circ\tau)(z)=\sigma(\tau(z))\in X$

  $(\sigma|_X\circ\tau|_X)(z)=\sigma|_X(\tau(z))=\sigma(\tau(z))$
- $\ker\varphi=\{\sigma\in G(E/R)\mid\varphi(\sigma)=\sigma|_X=1_X\}=\{1_E\}$

Definition 5.

① E is a pure extension of type m of k

$\Leftrightarrow$ $E=k(u)$ where $u^m\in k,\ m\geq 1$

② K : radical extension of k

$\Leftrightarrow$ $\exists\, k=K_0\subset K_1\subset K_2\subset\cdots\subset K_Z=K$

where each K_{i+1} is a pure extension of K_i

Example 7.

$x^m-a\in\mathbb{Q}[x]$

$\exists\, u$ s.t. $u^m=a$

let $w=e^{2\pi i/m}$

then $\{u,\ uw,\ uw^2,\cdots,\ uw^{n-1}\}=X$

Definition 6.

$f(x)\in k[x]$, E is the splitting field of $f(x)$ over k

$f(x)$ is solvable by radicals

$\Leftrightarrow$ $\exists$ radical extension

$k=K_0\subset K_1\subset\cdots\subset K_i$ s.t. $E\subset K_i$

Theorem 23.

$k\subset K\subset E$ are field towers, $f(x),\ g(x)\in k[x]$

K is the splitting of $f(x)$, E is the splitting of $g(x)$

$\Rightarrow$ ① $G(E/K)\lhd G(E/k)$

② $G(E/k)/G(E/K) \cong G(K/k)$

E
|
K
|
k

proof :

Define $\varphi : G(E/k) \to G(K/k),\ \varphi(\sigma) = \sigma|_K$ then

① $\varphi(\sigma) = \sigma|_K$: well defined

② φ : homomorphism.

③ $\ker\varphi = G(E/k)$

④ φ : surjective $\quad \because\ \tau \in G(K/k) \ \Rightarrow\ \exists\, \bar{\tau} \in G(E/k)$ s.t. $\bar{\tau}|_K = \tau$

Definition 7.

G : group

G : solvable $\Leftrightarrow\ \exists\, G = G_0 \supset G_1 \supset \cdots \supset G_n = \{e\}$

s.t. $G_i \lhd G_i,\ G_{i-1}/G_i$: Abel group

Example 8.

S_4 : solvable

$S_4 \supset A_4 \supset V \supset W \supset \{e\}$

$A_4 \lhd V$ (A_4, V를 구체적으로 찾아서 보이시오.)

But S_5 : not solvable

$\because\ S_5 \lhd A_5 \lhd \{e\}$ ← S_5의 normal chain은 이것밖에 없는데

A_5, S_5 : simple group이므로

$A_5/\{e\} \cong A_5$ ← not Abel.

Theorem 24.

$n \geq 5$

$f(x) = (x-y_1)(x-y_2)\cdots(x-y_n)$ where $y_1, y_2, \cdots, y_n \in \mathbb{C}$

$= x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Q}[x]$

the splitting field of $f(x)$ over $\mathbb{Q} = \mathbb{Q}(y_1, y_2, \cdots, y_n) = E$

$G(E/\mathbb{Q}) \cong S_n$: not solvable

<연습문제>

1. Express $x^8 - x$ as a product of irreducible over Z_2.

2. Let $f(x)$ be a nonzero element of $F[x]$. If a belongs to some extension of F and $f(a)$ is algebraic over F, Prove that a is algebraic over F.

3. Let a be a complex zero of $x^2 + x + 1$ over Q.
Prove that $Q(\sqrt{a}) = Q(a)$.

4. If $f(x)$ is a cubic irreducible polynomial over Z_3, prove that either x or $2x$ is a generator for the cyclic group $Z_{3[x]}/ < f(x) >$.

5. Let R be an integral domain that contains a field F as a subring.
If k is finite-dimensional when viewed as a vector space over F, prove that R is a field.

6. Prove that a 40° angle is not construable.

7-8. Let E be the splitting field of $x^4 + 1$over Q. Find $Gal(E/Q)$. Find all subfields of E. Find the automorphism of E that have fixed fields $Q(\sqrt{2})$ and $Q(i)$.

9. Let w be a nonreal complex number such that $w^5 = 1$. If ϕ is the automorphism of $Q(w)$ that carries w to w^4, find the fixed field of $< \phi >$.

10. This exercise exhibits a polynomial of degree 5 in Q[x] that is not solvable by radicals over Q.
a. Show that if a subgroup H of S_5 contains a cycle of length 5 and a transposition τ, then $H = S_5$.
b. Show that if $f(x)$ is an irreducible polynomial in $Q[x]$ of degree 5 having exactly two complex and three real zeros in C, then the group of $f(x)$ over Q is isomorphic toS_5.
c. The polynomial $f(x) = 2x^2 - 5x^4 + 5$ is irreducible in $Q[x]$, by the Eisenstein criterion, with $p = 5$. Use the techniques of calculus to find relative maxima and minima and to see that $f(x)$ must have exactly three real zeros in C. Conclude from part (b) $f(x)$ is not solvable by radicals over Q.