Prop 13.
If H and K are finites subgroup of a group then,

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$$

proof)
Think of the collection of coset,

$$\mathcal{A} = \{hK ; h \in H\}$$

then, h_1K meets h_2K iff $h_1 \cdot h_2^{-1} \in K$ and moreover, when if this holds $h_1K = h_2K$.

Since $\forall h \in H \cap K.\ h_1 \cdot h \in H$ holds, the number of disjoint sets in $\mathcal{A}$ is $\frac{|H|}{|H \cap K|}$

Therefore, $|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$.

Prop 14
If H and K are subgroup of a group, HK is a subgroup iff $HK = KH$.
proof)
($\Rightarrow$) Let $h \in H$, $k \in K$.

$$(h \cdot k) \cdot (h^{-1} \cdot k^{-1}) = id.$$

$$hk = k \cdot h.$$

Thus, $HK = KH$ holds.

($\Leftarrow$) $\forall x, y \in HK$, $\exists z \in KH$, $y^{-1} = z$ holds.

$$x \cdot y^{-1} = x \cdot z$$

$$= (x_h \cdot x_k)(z_k \cdot z_h)$$

$$= x_h (x_k \cdot z_k \cdot z_h)$$

$$\in x_h\, KH = x_h \cdot HK = H \cdot K$$

KOKUYO LOOSE-LEAF ノ-836BT 6 mm ruled x 36 lines

Thus, HK form the subgroup.

Cor 15

If H and K are subgroups of G and $H \leq N_G(K)$, then $H \cdot K$ is a subgroup of G.

In particular, if $K \trianglelefteq G$, then $HK < G$ for any $H \leq G$.

Proof)

We assert $H \leq N_G(K)$ implies $HK = KH$.

$\forall x \in HK$, $\exists h, k$ $x = h \cdot k$ since $H \leq N_G(K)$ holds, $hkh^{-1} = k$.

Thus, $x = k \cdot h \in KH$

Similaly, $HK \supset KH$. Thus, $H \cdot K$ form the subgroup.

Let $K \trianglelefteq G$, $H \leq G$.

$\forall x, y \in HK$

$$x \cdot y^{-1} = (x_h \cdot x_k) \cdot (y_k^{-1} \cdot y_h^{-1}) = x_h (y_h^{-1} \cdot y_h)(x_k \cdot y_k^{-1}) \cdot y_h^{-1}$$

$$= z_h \cdot z_k \in H \cdot K$$

Since $K \trianglelefteq G$, $y_h (x_k \cdot y_k^{-1}) \cdot y_h^{-1} \in K$, we can pick $z_k = y_h (x_k \cdot y_k^{-1}) y_h^{-1}$

and $z_h = x_h \cdot y_h^{-1}$

Thm 16. The first isomorphism theorem.

If $\varphi : G \to H$ is a homomorphism of groups, then $\ker\varphi \trianglelefteq G$ and $G/\ker\varphi \simeq \varphi(G)$.

proof)

Clearly $\ker\varphi$ form a subgroup of G.

$\forall x \in \ker\varphi$, $\forall g \in G$.

$$\varphi(g \cdot x \cdot g^{-1}) = \varphi(g) \cdot \varphi(x) \cdot \varphi(g^{-1})$$

$$= \varphi(g \cdot g^{-1})$$

$$= id.$$

Thus, $g \cdot x \cdot g^{-1} \in \ker \varphi$ and therefore $\ker \varphi \trianglelefteq G$.

$\varphi : G/\ker\varphi \to \varphi(G)$ is clearly bijective and homomorphism.

Cor 17.
Let $\varphi : G \to H$ be a homomorphism of groups.

(1) φ is injective iff $\ker \varphi = id$,

(2) $|G : \ker \varphi| = |\varphi(G)|$.

Proof.)
(1) ($\Rightarrow$) Since, φ is injective, clearly $\ker \varphi$ be a singleton, written a.

For every $g \in G$,

$$\begin{cases} \varphi(g \circ a) = \varphi(g) \cdot \varphi(a) = \varphi(g) \\ \varphi(a \circ g) = \varphi(a) \cdot \varphi(g) = \varphi(g) \end{cases} \quad \text{holds.}$$

Thus, $a = id$ therefore, $\ker \varphi = id$.

($\Leftarrow$) Suppose we can pick distinct x, y from G

$$\varphi(x \circ y^{-1}) = \varphi(x) \cdot \varphi(y^{-1})$$

$$= \varphi(x) \cdot \varphi(y)^{-1}$$

Since, $x \neq y$, $x \circ y^{-1} \neq id$ thus, by $\ker \varphi = id$, $\varphi(x) \cdot \varphi(y)^{-1} \neq id$.

KOKUYO LOOSE-LEAF ノ-836BT 6 mm ruled×36 lines

Thus, $\varphi(x) \neq \varphi(y)$, φ is injective.

(2) By previous theorem.

Thm 18 The Secound or Diamond Isomorphism Theorem.

Let G be a group, let A and B be subgroups of G and assume $A \leq N_G(B)$.

Then AB is a subgroup of G, $B \trianglelefteq AB$, $A \cap B \trianglelefteq A$ and $AB/B \simeq A/A \cap B$.

Proof).

By 14, 15, AB form the subgroup and $AB = BA$.

$\forall b \in B, \forall a', b' \in AB, \exists b'', a'' \in BA$ with $a' \cdot b' = b'' \cdot a''$.

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

$$\in AB.$$

Thus, $B \trianglelefteq AB$.

$\forall b \in A \cap B, \forall a \in A$ by $B \trianglelefteq AB$, $(a \cdot 1) \cdot b (a \cdot 1)^{-1} \in B$,

and clearly $a \cdot b \cdot a^{-1} \in A$. Thus, $A \cap B \trianglelefteq A$.

Let $\varphi : A \to AB/B ; a \mapsto aB$. Then clearly φ is homomorphism,

and $\varphi^{-1}(B) = A \cap B$ thus, $A/A \cap B \simeq AB/B$.

Thm 19 The Third Isomorphism Theorem

Let G be a group and let H and K be normal subgroup of G with $H \leq K$.

Then $K/H \trianglelefteq G/H$ and $(G/H)/(K/H) \simeq G/K$.

proof.)

First to show for every $k \in K$ and $g \in G$,

$$(gH)(kH)(gH)^{-1} \in K/H.$$

By definition, $(gH)(kH)(gH)^{-1} = (g \cdot k \cdot g^{-1})H$ and since K is normal, $gkg^{-1} \in K$. Thus, $K/H \trianglelefteq G/H$.

Since, $H \leq K$, we can define the function φ as follows;

$$\varphi : G/H \to G/K \; ; gH \mapsto gK.$$

If we show $K/H = \ker\varphi$, by the first isomorphism theorem complete the proof.

However,

$$\ker\varphi = \{kH ; k \in K\} = K/H \text{ holds.}$$

Thm 2.0 The fourth or Lattice Isomorphism Theorem.

Let G be a group and let N be a normal subgroup of G. Then there is a bijection from the set of subgroups A of G which include N onto the set of subgroup A/N of G/N. In particular, every subgroup of $\overline{G}$ is of the form A/N for some subgroup A of G containing N. This bijection has the following properties : for all $A, B \leq G$ with $N \leq A$ and $N \leq B$.

(1) $A \leq B$ iff $\overline{A} \leq \overline{B}$,

(2) if $A \leq B$ then, $|B : A| = |\overline{B} : \overline{A}|$,

(3) $\overline{\langle A, B \rangle} = \langle \overline{A}, \overline{B} \rangle$ and,

(4) $A \trianglelefteq G$ iff $\overline{A} \trianglelefteq \overline{G}$.

KOKUYO LOOSE-LEAF ノ-836BT 6 mm ruled×36 lines

proof.)

If $A \neq B$ with $N \leq A, B$.

Then there exists b, $b \notin A$, $b \notin B$ moreover, $bN \notin A/N$ thus, the function is injective, and therefore, bijective.

(1) ($\Rightarrow$) For every a in A, a contained in B, thus $aN \in BN$ and therefore,

$A/N \leq B/N$.

($\Leftarrow$) For every a in A there exists some b in B such that $aN = bN$ moreover, there exists $n \in N$ such that $a = bn$. Since, $N \leq B$, $a \in B$.

Thus, $A \leq B$ and therefore, $A \leq B$.

(2) First we verify for $b_1, b_2 \in B$. if b_1N meets b_2N then $b_1N = b_2N$.

Since, b_1N meets b_2N, $\exists n, m \in N$ $b_1n = b_2m$ holds.

Moreover, $b_2 \in (b_1 \cdot a_1 \cdot a_2^{-1}) \in b_1N$ and therefore $b_1N = b_2N$.

By previous fact, we can define a function φ independent of choice;

$\varphi : \bar{B} \to B/A$; $bN \mapsto bA$

Then, clearly φ is homomorphism and $\ker\varphi = \bar{A}$.

Hence, $\bar{B}/\bar{A} \approx B/A$

(3) Let H be a subgroup with $\bar{A} \cup \bar{B} \leq \bar{H}$ then $\bar{A} \leq \bar{H}$ and $\bar{B} \leq \bar{H}$.

By (1), $A \leq H$, $B \leq H$ holds. Thus, $\langle A, B \rangle \leq H$, $\overline{\langle A, B \rangle} \leq \bar{H}$.

Therefore, $\overline{\langle A, B \rangle} \leq \langle \bar{A}, \bar{B} \rangle$ holds.

Let H be a subgroup with $\overline{\langle A,B\rangle} \leq \overline{H}$. then by (1) $\langle A,B\rangle \leq H$, then $A \leq H$ and $B \leq H$.

moreover, $\bar{A} \leq \overline{H}$ and $\bar{B} \leq \overline{H}$. Then, $\langle \bar{A}, \bar{B} \rangle \leq \overline{H}$.

Hence, $\langle \bar{A}, \bar{B} \rangle \leq \overline{\langle A,B\rangle}$.

Therefore, $\langle \bar{A}, \bar{B} \rangle = \overline{\langle A,B\rangle}$.

(5) ($\Rightarrow$) $\forall a, g$ we verify $(gN)(aN)(gN)^{-1} \in \bar{A}$.

Since $A \trianglelefteq G$, $(g \cdot a \cdot g^{-1})N \in \bar{A}$ and, $(gN)(aN)(gN)^{-1} = (g \cdot a \cdot g^{-1})N$ holds,

$(gN)(aN)(gN)^{-1} \in \bar{A}$.

($\Leftarrow$) $\forall a, g$. we verify $g \cdot a \cdot g^{-1} \in A$.

Since, $(gN)(aN)(gN)^{-1} \in \bar{A}$, $\exists a' \in A$, $g a g^{-1} = a'$ holds.

Thus, $g \cdot a \cdot g^{-1} \in A$ holds.

Prop 21 If G is a finite Abelian group and p is a prime dividing $|G|$, then G contains an element of order p.

Proof) By Cauchy's theorem it is clear.

Thm 22 Jordan - Hölder

Let G be a finite group with $G \neq id$. Then

(1) G has a composition series and

(2) The composition factors in a composition series are unique.

KOKUYO LOOSE-LEAF シ-836BT 6 mm ruled x36 lines

Lemma. Let G be a group, and let A and B be subgroup of G then,

B/A is simple iff A is maximal normal subgroup of B.

Proof).

($\Rightarrow$) Suppose A is not maximal normal subgroup, then there exists H such that $A \lneq H \trianglelefteq B$ moreover, $H/A \trianglelefteq B/A$ thus. $H = B$ or A a contradictions.

($\Leftarrow$) Suppose B/A is not simple, there exists $H \leq G$ such that $A < H \leq B$ and $H/A \lneq B/A$ thus, $\forall b \in B, \forall h \in H \quad bhb^{-1} \in H$ holds. Thus, H form the normal subgroup of B and moreover since A is maximal normal subgroup of B, $A \neq H$ a contradictions.

Proof). Jordan - Hölder.

(1) We prove by induction on $|G| \geq 2$.

If $|G| = 2$, clearly holds.

Assume there exists composition series of order less than $|G|$.

Let G_1 be maximal normal subgroup then, by assumption, G_1 posesses a composition series $G_1 > G_2 > \cdots > G_r = 1$ moreover by lemma $G > G_1 > \cdots > G_r = 1$ is the composition series of G.

Thus, every finite group possesses composition series.

(2) Let $G = G_0 > G_1 > \cdots > G_r = id$ ------ ①

be composition series of G. We prove by induction on r.

If $r=1$ then G is simple, thus by previous lemma, the composition factors are unique.

Let,

$$G = G_0 > H_1 > \cdots > H_s = id \quad \cdots ②$$

be composition series of G.

Assume, the composition factors, of every composition series with length less than r, are unique.

If $H_1 = G_1$, by assumption, the composition factors of H_1 and G_1 are unique and also $G_0/H_1 = G_0/G_1$ holds. Hence, the composition factors of ① and ② are the same.

If $H_1 \neq G_1$, since G_1 is normal, $H_1 \cdot G_1$ form the group and let $K_2 = H_1 \cap G_1$ then, $K_1 \trianglelefteq G$. Moreover, by Second Isomorphism Theorem, we obtain, $G_1/K_1 \cong G/H_1$ and $H_1/K_2 \cong G/G_1$, and since G/G_1 and G/H_1 are simple, G_1/K_1 and H_1/K_1 is also simple.

By (1) K_2 possesses composition series $K_2 > K_3 > \cdots > K_\ell = id$, moreover,

$$G_1 > K_2 > \cdots > K_\ell = id \quad \cdots ③ \text{ and}$$

$$H_1 > K_2 > \cdots > K_\ell = id \quad \cdots ④$$

form the composition series of G_1 and H_1.

By assumption, the composition factors of ③ are unique thus $r=\ell$, this implies the composition factors of ④ is also unique thus $\ell = s$.

This fact shows,

$$\{G_i/G_{i+1} ; 1 \le i \le r-1\} = \{G_1/K_2, K_i/K_{i+1} ; 2 \le i \le r-1\} \quad \cdots\cdots (*)$$

$$\{H_i/H_{i+1} ; 1 \le i \le r-1\} = \{H_1/K_2, K_i/K_{i+1} ; 2 \le i \le r-1\} \quad \cdots\cdots (**)$$

Hence,

$$\{G_i/G_{i+1} ; 0 \le i \le r-1\} \overset{(*)}{=} \{G_0/G_1, G_1/K_1, K_i/K_{i+1} ; 2 \le i \le r-1\}$$

$$\overset{\text{second Iso}}{=} \{H_1/K_2, G_0/H_1, K_i/K_{i+1} ; 2 \le i \le r-1\}$$

$$\overset{(**)}{=} \{G/H_1, H_i/H_{i+1} ; 1 \le i \le r-1\}.$$

Thus, the composition factors of composition series of G are unique.

Prop 1. For any group G and any non-empty set A there is a bijection between the actions of G on A and the homomorphisms of G into S_A.

Proof.)

Let Ψ be a function as follows;

$$\Psi : (\varphi : G \to S_A \,;\, g \mapsto \sigma_g) \mapsto (g \cdot a \mapsto \sigma_g(a))$$

Let φ, ψ be distinct homomorphism of G into S_A, then there exists $g_1 \in G$ such that $\varphi(g_1) \neq \psi(g_1)$.

This implies, there exists at least one pair of a and g such that $\varphi(g) \cdot a \neq \psi(g) \cdot a$ holds, thus Ψ is injective.

Let $\alpha : G \times A \to A$ be an action, define the function,

$$\varphi : g \longmapsto (a \mapsto \alpha(g, a) \,;\, a \in A).$$

Since, α is an action, $a \mapsto \alpha(g, a) \,;\, a \in A$ be a permutation on A.

We verify φ is homomorphism.

$$\forall g_1, g_2 \in G, \quad \varphi(g_1 \cdot g_2) = a \mapsto \alpha(g_1 \cdot g_2, a)$$
$$= a \mapsto \alpha(g_1, \alpha(g_2, a))$$
$$= \varphi(g_1) \circ \varphi(g_2).$$

Thus, φ is homomorphism and therefore Ψ is surjective.

KOKUYO LOOSE-LEAF J-836BT 6 mm ruled×36 lines

Prop 2. Let G be a group acting on the nonempty set A. The relation on A defined by $a \sim b$ iff $a = g \cdot b$ for some $g \in G$ is an equivalent relation. For each $a \in A$, the number of elements in the equivalence class containing a is $|G : G_a|$, the index of the stabilizer of a.

Proof). The relation is an equivalent class is clear.

Let $g_1, g_2 \in G$ such that $b = g_1 a$, $b = g_2 a$ holds.

We verify, $g_1 \cdot G_a = g_2 \cdot G_a$ ..... (*)

Since $g_1 a = g_2 a$, $g_1^{-1} \cdot g_2 a = a$ holds, and for each $g \in G_a$ $ga = a$.

Thus, $ga = g_1^{-1} \cdot g_2 \cdot a$, $g_2^{-1} \cdot g_1 \cdot g \cdot a = a$,

moreover, $g_2^{-1} \cdot g_1 \cdot g \in G_a$ and, $g_2 (g_2^{-1} \cdot g_1 \cdot g) = g_1 \cdot g$ holds.

Hence, $g_1 \cdot G_a \subset g_2 \cdot G_a$, in similar way $g_1 \cdot G_a \supset g_2 \cdot G_a$.

Therefore $g_1 \cdot G_a = g_2 \cdot G_a$ holds.

Let φ be the function as follows;

$$b \longmapsto g_b \cdot G_a \quad \text{where} \quad b \sim a \text{ and } b = g_b \cdot a.$$

By (*), φ is independent of the choice of b.

Let $b = g_b \cdot a$ and $c = g_c \cdot a$ and suppose $g_b G_a = g_c G_a$ holds.

Then there exists $g \in G_a$ such that $g_b = g_c \cdot g$ holds,

moreover, $g_b \cdot a = g_c \cdot g \cdot a = g_c \cdot a$ thus $b = c$.

Therefore, φ is injective and clearly φ is surjective.

Thus, φ be the bijection from equivalent class of a into $\{gGa\}$

Thm 3. Let G be a group, let H be a subgroup of G and let G act by left multiplication on the set A of left cosets of H in G. Let π_H be the associated permutation representation afforded by this action. Then

(1) G acts transitively on A,

(2) the stabilizer in G of the point $1H \in A$ is the subgroup H,

(3) the kernel of the action is $\bigcap_{x \in G} xHx^{-1}$, and $\ker \pi_H$ is the largest normal subgroup of G included H.

Proof.)

(1) We show for $g_1H, g_2H \in A$, $\{g \cdot g_1H ; g \in G\} = \{g \cdot g_2H ; g \in G\}$ holds.

For arbitrary $g \in G$, we can pick $g \cdot g_1 \cdot g_2^{-1} \in G$ then,

$g \cdot g_1H = (g \cdot g_1 \cdot g_2^{-1})(g_2H)$ holds and therefore, the action is transitive.

(2) By definition,

$$G_{1H} = \{g ; gH = 1H\}$$
$$= \{g ; gH = H\}$$
$$= H \quad \text{holds.}$$

KOKUYO LOOSE-LEAF ノ-836BT 6 mm ruled x 36 lines

(3)

$$\ker \pi_H = \{g \in G ;\ g \cdot g'H = g'H \text{ for all } g' \in G\}$$

$$= \{g \in G ;\ \forall g' \in G\ \ g'^{-1} \cdot g \cdot g' \in H\}$$

$$= \{g \in G ;\ \forall g' \in G ,\ g \in g'Hg'^{-1}\}$$

$$= \bigcap_{g' \in G} g'Hg'^{-1}.$$

And clearly, $\ker \pi_H \subset H$ and $\ker \pi_H \trianglelefteq G$.

Let N be a normal subgroup of G included H,

then, $N = \bigcap_{g' \in G} g'Ng'^{-1} \subseteq \bigcap_{g' \in G} g'Hg'^{-1}$ holds.

Hence, $\ker \pi_H$ is the largest normal subgroup of G included H.

Cor 4. Cayley's Theorem

Every group is isomorphic to a subgroup of some symetric group.

Proof.)

For Thm 3. put $H = id$ then by prop1 there exists isomorphism from G to S_G moreover since $\ker \subseteq id$. G is isomorphic to subgroup of S_G.

Cor 5 If G is a finite group of order n and p is the smallest prime divising $|G|$, then any subgroup of index p is normal.

Proof)

Let $H \leq G$, $|G : H| = p$, and let π_H is the permutation representation induced by left cosets of H in G.

Since H has p left coset, $G/\ker\pi_H$ is isomorphic to subgroup of S_p.

Let $|H : \ker\pi_H| = k$ then,

$|G : \ker\pi_H| = |G : H| \cdot |H : \ker\pi_H| = pk$ holds.

Since, $|S_p| = p!$, by Lagrange's Theorem, $pk = |G/\ker\pi_H|$ divides $p!$

Thus. $k \mid \frac{p!}{p}$, $k \mid (p-1)!$ holds.

Since, $\exists l$: prime, $k = l \cdot k'$, $k' \in \mathbb{Z}$ holds, $|G| = |\ker| \cdot pk = |\ker| \cdot p \cdot l \cdot k$, $l \mid |G|$.

However, since $k \mid (p-1)!$ holds, k has no prime divisor, $k = 1$.

Thus. $H = \ker\pi_H$ and therefore H be a normal subgroup.

Prop 6. The number of conjugates of a subset S in a group G is the index of the normalizer of S, $|G : N_G(S)|$. In particular, the number of conjugates of an element s of G is the index of the normalizer of s, $|G : C_G(s)|$.

Proof.)

Let, $\mathcal{C} = \{A \mid A$ is conjugate of S by some $g \in G\}$

We assert for $A \in \mathcal{C}$, $g_1, g_2 \in G$ if $A = g_1 \cdot S \cdot g_1^{-1}$ and $A = g_2 \cdot S \cdot g_2^{-1}$ holds, then, $g_1 N_G(S) = g_2 N_G(S)$ holds. .... (*)

$\forall g \in N_G(S)$

Since, $g \cdot S \cdot g^{-1} = S$ holds, $(g_1 \cdot g)\, S\, (g_1 \cdot g)^{-1} = A$ holds,

moreover, $(g_2^{-1} \cdot g_1 \cdot g)\, S\, (g_2^{-1} \cdot g_1 \cdot g) = S$, $g_2^{-1} \cdot g_1 \cdot g \in N_G(S)$ and,

$g_2 (g_2^{-1} g_1 \cdot g)$ holds, $g_1 N_G(g) \subset g_2 \cdot N_G(S)$.

KOKUYO LOOSE-LEAF J-836BT 6 mm ruled×36 lines

Similarly, $g_1 N_G(S) \supset g_1 \cdot N_G(S)$ holds, thus, $g_1 N_G(S) = g_2 \cdot N_G(S)$.

By (*) we can define the function independent of choice,

$$\varphi : \mathbb{G} \to \{g N_G(S)\} \; ; \; A \mapsto g_A \cdot N_G(S) \text{ where } A = g_A \cdot S \cdot g_A^{-1}$$

Clearly, φ is surjective, thus verify φ is injection.

Let $A, B \in \mathbb{G}$ and $\varphi(A) = \varphi(B)$.

Then there exists g_A, g_B such that $A = g_A \cdot S \cdot g_A^{-1}$, $B = g_B \cdot S \cdot g_B^{-1}$

and since, $g_A \cdot N_G(S) = g_B \cdot N_G(S)$, there exists $g \in N_G(S)$ such that

$g_A = g_B \cdot g$ holds.

For all $a \in A$, $a \in g_A \cdot S \cdot g_A^{-1} = g_B (g \cdot S \cdot g^{-1}) \cdot g_B^{-1} = g_B \cdot S \cdot g_B^{-1} = B$

thus, $A \subset B$, similarly $A \supset B$. Thus $A = B$, φ is injective.

Thm7. The class Equation

Let G be a finite group and let $g_1, \cdots, g_r$ be representatives of the distinct conjugacy class of G not contained in the center $Z(G)$ of G. Then,

$$|G| = |Z(G)| + \sum_{k=1}^{r} |G : C_G(g_i)|$$

Proof)

First, we show if $x \in Z(G)$, the conjugate class of x is $\{x\}$.

Let C_x be the class of x. $\forall y \in C_x$. $\exists g \in G$. $y = g \cdot x \cdot g^{-1}$. Since $x \in Z(G)$,

$gx \cdot g^{-1} = x$ holds, thus $y = x$ then, $C_x = \{x\}$.

By prop 6. $|G : C_G(g_i)|$ is equals to the number of equivalent class

of g_i. Hence, $|G| = |Z(G)| + \sum_{1 \le i \le r} |G : C_G(g_i)|$ holds.

Thm 8. If p is prime and P is a group of prime power order p^α for some $\alpha \ge 1$, then P has nontrivial center : $Z(P) = 1$.

Proof)

By prop 7, $|P| = |Z(P)| + \sum_{1 \le i \le r} |P : C_P(g_i)|$ where g_i is representatives of the distinct conjugacy class of G not contained $Z(P)$. thus, $C_P(g_i) \neq P$ for all i.

Since, $C_P(g_i)$ is subgroup of P, p divides $|P : C_P(g_i)|$.

Thus, p divies. $\sum |P : C_P(g_i)|$, moreover, p divies $Z(P)$ this shows there exists non-trivial center.

Cor 9. If $|P| = p^2$ for some pime p, then P is Abelian. More precisely, P is isomorphic to either $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$.

Proof)

By Thm 8. $Z(P) \neq 1$ thus, $|Z(P)| = p$ or p^2 thus, $P/Z(P)$ is cyclic.

Now, We assert ingenerally, if $G/Z(G)$ is cyclic, then G is an Abelian.

$\forall x, y \in G$. $\exists a_1, a_2 \in \mathbb{Z}$, $z_1, z_2 \in Z(G)$ and α, such that

$x = \alpha^{a_1} z_1$, $y = \alpha^{a_2} \cdot z_2$ holds.

Then, $x \cdot y = (\alpha^{a_1} \cdot z_1) \cdot (\alpha^{a_2} \cdot z_2) = (\alpha^{a_1} \cdot \alpha^{a_2} \cdot z_1 \cdot z_2)$

$= \alpha^{a_1 + a_2} \cdot z_2 \cdot z_1 = y \cdot x$, and therefore G is an Abelian.

KOKUYO LOOSE-LEAF

Hence, P is an Abelian.

Since, P has an element with order p^2, Then P is cyclic, $P \approx \mathbb{Z}_{p^2}$.

If every non-identity element is order p, let $x \in P \setminus id$, $y \in P \setminus \langle x \rangle$.

By, $|\langle x, y \rangle| > |\langle x \rangle| = p$, $|\langle x, y \rangle| = p^2$, $P = \langle x, y \rangle$,

and we can define the isomorphism;

$$\langle x^n, y^m \rangle \longmapsto \langle n, m \rangle$$

This show $P \approx \mathbb{Z}_p \times \mathbb{Z}_p$.

Prop10. Let σ, τ be elements of the symetric group S_n and suppose σ has cycle decomposition $(a_1\ a_2 \cdots a_{k_1})(b_1\ b_2 \cdots b_{k_2}) \cdots$.

Then, $\tau\sigma\tau^{-1}$ has cycle decomposition

$$(\tau(a_1)\ \tau(a_2) \cdots \tau(a_{k_1}))(\tau(b_1)\ \tau(b_2) \cdots \tau(b_{k_2})) \cdots,$$

that is, $\tau\sigma\tau^{-1}$ is obtained from σ by replacing each entry i in the cycle decomposition for σ by entry $\tau(i)$.

Proof)

We assert if $\sigma(i) = j$ then $\tau\sigma\tau^{-1}(\tau(i)) = \tau(j)$ holds.

Thus, if the ordered pair i, j appears in the cycle decompositon of σ, then the ordered pair $\tau(i), \tau(j)$ appear in the cycle decomposition of $\tau\sigma\tau^{-1}$.

This complete the proof.

Thm 12 A_5 is a simple group.

Proof) At the beginning of the proof we assert the following:

Let $\sigma, \tau \in S_n$ and $F_\sigma := \{ i ; \sigma_i = i \}$. Then $\tau\sigma = \sigma\tau$ implies $\tau(F_\sigma) = F_\sigma$ and moreover if σ is n-cycle, $\tau = \sigma^i$ for some i.

Since, the first assertion is clear, we prove that "moreover" part.

Fix $a_0 = 1$ and since σ is n-cycle, $\sigma = (a_0\ a_1 \cdots a_{n-1})$. Since τ has a fixed point, we obtain $\tau = id = \sigma^0$ so assume that τ does not possesses fixed points.

Let $\tau(1) = a_i\ (\neq 1)$ then we have $\tau(a_k) = a_{k+i}$ by induction, so. $\tau = \sigma^i$.

Next, we verify the representation for each conjugacy class is id, (123), (12)(34), (12345), (14325) by calculate the number of the elements in each conjugacy class. Note that by prop 6, the number of elements is equal the order of A_5 divide by the order of its centlizer.

(i) id. The number of the elements in conjugacy class for id is clearly 1.

(ii) (123).

For $\sigma \in S_5$. If $\sigma \in C_{S_5}(123)$, i.e., $\sigma(123) = (123)\sigma$ by above assertion, $\sigma : \{4,5\} \to \{4,5\}$ and moreover, $\sigma|_{\{1,2,3\}}(123) = (123)|_{\sigma\{1,2,3\}}$ holds in S_3 and (123) is 3-cycle, $\sigma|_{\{1,2,3\}} = (123)^i$. i.e., $\sigma|_{\{1,2,3\}} = id, (123), (132)$ and since we have $\sigma|_{\{4,5\}} = id, (4,5)$. We can determine $C_{A_5}(123) = \{ id, (123), (132) \}$, so the number of the elements in conjugacy class for (123) is $\frac{60}{3} = 20$.

KOKUYO LOOSE-LEAF ノ-836BT 6 mm ruled×36 lines

(iii) $(12)(34)$.

For $\sigma \in S_5$. If $\sigma \in C_{S_5}(12)(34)$, i.e., $\sigma(12)(34) = (12)(34)\sigma$, since $(12)(34) : \{5\} \to \{5\}$,

$$\sigma : \{1,2,3,4\} \longrightarrow \{1,2,3,4\}$$

A σ in S_4 is the form id, (12), $(12)(23)$, $(12)(34)$ however, $((12)(23))((12)(34)) \neq ((12)(34))((12)(23))$, we consider the following σ in A_5, id, $(12)(34)$, $(13)(24)$, $(14)(23)$ and all of them satisfies $\sigma(12)(34) = (12)(34)\sigma$. Thus, $C_{A_5}(12)(34) = \{id, (12)(34), (13)(24), (14)(23)\}$.

Thus, the number of elements in conjugacy class for $(12)(34)$ is $\frac{60}{4} = 15$.

(iv) (12345)

For $\sigma \in S_5$. If $\sigma \in C_{S_5}(12345)$, $\sigma = (12345)^2$, i.e., $\{id, (12345), (13524), (14253), (15432)\}$ and all of them in A_5. So the number of the elements in conjugacy class of (12345) is $\frac{60}{5} = 12$.

(v) (14325)

Similaly to the case (iv), $C_{A_5}(14325) = \{id, (14325), (13542), (12453), (15234)\}$. So the number of the elements in conjugate class of (14325) is $\frac{60}{5} = 12$.

Therefore, the list of the number of elements of each conjugacy class is $1, 20, 15, 12, 12$ and the sum is $60 (= |A_5|)$ so there are no more conjugate class.

Finally, a normal subgroup of A_5 is the union of conjugacy class so the possible order is $1, 13, 16, 21, 25, 28, 33, 35, 40, 45, 48$ or 60 and by Lagurage theorem, possible order for subgroup is, $1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30$ or 60. Therefore, the order of normal subgroup of A_5 is 1 or 60, i.e., A_5 is simple.

Prop13. Let H be a normal subgroup of the group G. Then G acts by conjugation on H as automorphism of H. More specifically the action of G on H by conjugation is defined for each $g \in G$ by $h \mapsto ghg^{-1}$ for each $h \in H$. For each $g \in G$, conjugation by g is an automorphism of H. The permutation representation afforded by this action is a homomorphism of G into $Aut(H)$ with kernel $C_G(H)$. In particular, $G/C_G(H)$ is isomorphic to a subgroup of $Aut(H)$.

Proof).

We verify, $h \mapsto ghg^{-1}$ for every g be an action.

Let $g_1, g_2 \in G$.

$g_1 \circ (g_2 \circ h) = g_1 \circ (g_2 h g_2^{-1}) = (g_1 \cdot g_2) \cdot h \cdot (g_1 \cdot g_2)^{-1} = (g_1 \cdot g_2) \circ h$,

$id \circ h = id \cdot h \cdot id^{-1} = h$.

Thus. $h \mapsto ghg^{-1}$ for every $g \in G$ form an action, moreover for every g, there exists some $\sigma_g \in S_H$ such that $\sigma_g(h) = ghg^{-1}$. Thus, $h \mapsto ghg^{-1}$ is an automorphism.

Let $\varphi : g \mapsto \sigma_g \in Aut(H)$ be a permutation representation, then φ is homomorphism.

Next, we verify. $\ker \varphi = C_G(H)$

$\forall g \in \ker \varphi$, since $\sigma_g = \varphi(g) = id$.

$\forall h \in H$, $h = \sigma_g(h)$ # $ghg^{-1} = h$ holds. Thus. $g \in C_G(H)$.

$\forall g \in C_G(H)$, for every $h \in H$, $ghg^{-1} = h$ holds.

Moreover $\varphi(g) = id$ and therefore $g \in \ker \varphi$.

Hence, $\ker \varphi = C_G(H)$ and $G/\ker \varphi \simeq \varphi(G) \leq Aut(H)$.

KOKUYO LOOSE-LEAF ノ-836B7 6 mm ruled × 30 lines

Cor 14. If K is any subgroup of the group G and $g \in G$, then $K \cong gKg^{-1}$. Conjugate elements and conjugate subgroup have same order.

Proof.)

Letting $H = G$ in previous proposition then conjugation by $g \in G$ is an automorphism of G.

Cor 15 For any subgroup H of a group G, the quotient group $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $Aut(H)$. In particular, $G/Z(G)$ is isomorphic to a subgroup of $Aut(G)$.

Proof.)

Since H is a normal subgroup of $N_G(H)$, by prop 13, $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $Aut(H)$.

And since, G is a normal subgroup of G, by prop 13, $G/C_G(G)$ is isomorphic to a subgroup of $Aut(G)$, and clearly $C_G(G) = Z(G)$ thus, $G/Z(G)$ is isomorphic to a subgroup of $Aut(G)$.

Prop 16. The automorphism group of the cyclic group of n is isomorphic $(\mathbb{Z}/n\mathbb{Z}, \times)$, an Abelian group of order says $\varphi(n)$.

Proof.)

Let $\langle x \rangle$ be n cyclic group, and let

$$f : Aut\langle x \rangle \longrightarrow \mathbb{Z}/n\mathbb{Z} \;;\; \varphi \mapsto a \text{ modulo } n,\ \varphi(x) = x^a \text{ holds.}$$

Since, $\varphi(x) = x^a$ holds, the automorphism φ is uniquely determines thus clearly f is surjective.

We verify f is homomorphism.

Let $\varphi, \psi \in Aut\langle x \rangle$ with $\varphi(x) = x^a$, $\psi(x) = x^b$.

$f(\varphi \circ \psi) = f((x^b)^a) = a \cdot b = f(\varphi) \cdot f(\psi)$ holds.

Thus. f is homomorphism and therefore, f is isomorphism.

KOKUYO LOOSE-LEAF ノ-836BT 6 mm ruled×36 lines

Lemma 19. Let $P \in Syl_p(G)$. If Q is any p-group of G, then $Q \cap N_G(P) = Q \cap P$.

Proof).

Since $P \leq N_G(P)$ holds, clearly $Q \cap P \leq Q \cap N_G(P)$.

And since $Q \cap N_G(P) \leq Q$ holds. We verify $Q \cap N_G(P) \leq P$.

Now, since $Q \cap N_G(P) \leq N_G(P)$ holds, by Sec 3.2 Cor 15, $P \cdot (Q \cap N_G(P))$ form the group and by Sec 3.2 Prop 13,

$$|P \cdot Q \cap N_G(P)| = \frac{|P| \cdot |Q \cap N_G(P)|}{|P \cap (Q \cap N_G(P))|} \text{ holds.}$$

Now, $|P|, |Q \cap N_G(P)|$ are power of p,

$|P| \cdot |Q \cap N_G(P)| \neq |P \cap Q \cap N_G(P)|$ holds, $P \cdot Q \cap N_G(P)$ is a p-subgroup and moreover, P is the subgroup of $P \cdot Q \cap N_G(P)$ and P is a Sylow p-subgroup thus, $P = P \cdot Q \cap N_G(P)$, $Q \cap N_G(P) \leq P$ holds, this comple the proof.

Thm 18 Sylow's theorem.

Let G be a group of order $p^d \cdot m$, where p is prime not dividing m.

(1) Sylow p-subgroup of G exists.

(2) If P is a Sylow p-subgroup of G and Q is any p-subgroup of G, then there exists $g \in G$ such that $Q \leq g \cdot P \cdot g^{-1}$. In paticular, any two Sylow p-subgroup of G are conjugate in G.

(3) The number of Sylow p-subgroup of G is of the form $1 + kp$. i.e,

$$n_p \equiv 1 \text{ modulo } p.$$

KOKUYO LOOSE-LEAF J-836BT 6 mm ruled x36 lines

Futher, n_p is the index in G of normalizer $N_G(P)$ for any Sylow p-subgroup P, hence n_p divides m.

Proof)

(1) We probe the proposition by induction on $|G|$ (≥ 2).

If $|G| = 2$ clearly holds.

Assume, every group of order less than $|G|$ has Sylow p-subgroup.

If $p \mid |Z(G)|$.

By Cauchy's theorem $Z(G)$ possesses a group N of order p, moreover $N \trianglelefteq G$ holds, $\therefore G/N$ form the group of order $p^{d-1} \cdot m$. Thus by assumption G/N possesses a Sylow p-subgroup such that $H/N \leq G/N$

If $p \nmid |Z(G)|$,

By class equation, there exists representatives of conjugate g_i which not in $Z(G)$ such that $p \nmid |G : C_G(g_i)|$. This implies $p^d \mid C_G(g_i)$ moreover $|C_G(g_i)| = p^d \cdot k$ for some k. And clearly $C_G(g_i) \lneq G$ thus by assumption $C_G(g_i)$ possesses Sylow p-subgroup.

Therefore, for every order of $|G|$, G possesses Sylow p-subgroup.

Before proving (2) and (3) we make some calculations.

Let P be a Sylow p-subgroup, define the collection S as follows;

$S = \{gPg^{-1}; g \in G\}$ written $S = \{P_1, \cdots, P_r\}$.

Let Q be a p-subgroup of G and let $\mathcal{O}_1, \cdots, \mathcal{O}_s$ be an orbit by act by conjugation on S,

$\mathcal{O}_i = \{gP_ig^{-1}; g \in Q\}$ for all $1 \le i \le s$.

Then clearly, $\cup \mathcal{O}_i = S$ and $r = \sum_{1 \le i \le s} |\mathcal{O}_i|$ holds.

Moreover by prop2,

$|\mathcal{O}_i| = |Q : G_{P_i}| = |Q : N_G(P_i)|$ holds.

And since,

$N_G(P_i) = N_G(P_i) \cap Q = P_i \cap Q$ holds,

$|\mathcal{O}_i| = |Q : P_i \cap Q|$ holds for $1 \le i \le s$ independent of p-subgroup Q ····(*)

Now, we verify $r \equiv 1$ modulo p. ·····(**)

It is enough to check the case of $Q = P_1$. Then clearly $\mathcal{O}_1 = 1$.

Now for $i > 1$, $P_1 \neq P_i$ implies $P_1 \cap P_i < P_i$. Then by (*)

$|\mathcal{O}_i| = |P_i : P_i \cap P_1| > 1$ for $2 \le i \le s$.

Moreovere since P is Sylow p-subgroup, $p \mid |\mathcal{O}_i|$ for all $2 \le i \le s$.

Thus, $r \equiv 1$ modulo p holds.

(2) Let Q be any p-subgroup,

KOKUYO LOOSE-LEAF ノ-836BT 6 mm ruled ×36 lines

Suppose Q does not contained P_i for any i.

Then $Q \cap P_i < Q$ for every i, moreover $|O_i| = |Q : Q \cap P_i| > 1$.

Thus, $p \mid |O_i|$ for every i, a contradictions.

Therefore $Q \leq gPg^{-1}$ for some g.

In paticular, if Q is Sylow p-subgroup, $|Q| = |gPg^{-1}|$ holds, thus $Q = gPg^{-1}$.

Therefore, any two Sylow p-subgroup is conjugate.

(3) By (2) and (**) clearly $n_p \equiv 1$ modulo p.

And by prop 6,

$n_p = |G : N_G(P)|$ for any $P \in Syl_p(G)$.

This complete the proof of Sylow's theorem.

Cor 20. Let P be a Sylow p-subgroup of G. Then the following are equivalent:

(1) P is the unique Sylow p-subgroup.

(2) P is normal in G.

(3) P is characteristic in G

(4) All subgroups generated by elements of p-power order are p-groups.

Proof.)

(1) $\Rightarrow$ (3) Let φ be an automorphism of G. Then $\varphi(P)$ form the Sylow p-subgroup

thus $\varphi(P) = P$.

(3) ⇒ (2)

For every $g_1 \in G$ define $\varphi : g \mapsto g_1 \cdot g \cdot g_1^{-1}$, then φ is an automorphism, $\varphi(P) = P$ holds. Therefore for every $p \in P$, $g_1 \cdot p \cdot g_1^{-1} \in P$ holds, hence P is normal in G.

(2) ⇒ (4).

Since G/P form the group of order m, by Cauchy's theorem if $g \in G$ does not in P, p does not devide the order gP thus, every element of p-power order contained in P. Thus the subgroups generated by elements of p-power order is the subgroup of P thus, p-subgroup.

(4) ⇒ (1)

Let $A := \cup \{gPg^{-1} ; g \in G\}$ then by assumption A is p-group thus, there exists $g_1 \in G$ such that $A \leq g_1 P g_1^{-1}$ moreover, $A = g_1 P g_1^{-1}$ holds thus, Sylow p-subgroup is unique.

KOKUYO LOOSE-LEAF ノ-836DT 6 mm ruled×36 lines

No.

Date

Thm 24 A_n is simple for all $n \geq 5$.

Proof) We prove by induction and the case A_5 is proved in thm 12.

Assume that there exists a nontrivial normal subgroup H of $A_n =: G$.

Define $G_i = \{\sigma \in G \mid \sigma(i) = i\}$ then $A_{n-1} \cong G_i \leq G$ so by induction hypothesis we have G_i is simple for every i.

First, we suppose that there exists nontrivial H such that $\tau(i) = i$ for some i.

Then since $\tau \in H \cap G_i$ we have $H \cap G_i \leq G_i$ i.e. $G_i \leq H$, for all $\sigma \in G$ and i we have $\sigma G_i \sigma^{-1}$ $= G_{\sigma(i)}$ and for every j there exists $\sigma \in G$ such that $\sigma(i) = j$ for fixed i, for every j, we have $G_j = G_{\sigma(i)} = \sigma G_i \sigma^{-1} \leq \sigma H \sigma^{-1} \leq H$, i.e., $G_j \leq H$ for all j. Let π, τ be transposition on S_n. Then, since $n > 4$, $\pi \circ \tau \in G_j$ for some j and for every π can be decompose by the product of even number of transpositions. Thus, $G = \langle G_j \mid j \rangle \leq H$, a contradiction.

Thus we obtain for every nontrivial τ in H, $\tau(i) \neq i$ for every i. Now, we assert for $\sigma, \tau \in H$ with $\sigma(i) = \tau(i)$, since $\tau^{-1}\sigma(i) = i$, i.e., $\tau^{-1}\sigma = id$, we have $\sigma = \tau$.

Second, we suppose there exists $\tau \in H$ with a form, cycle decomposition,

$$\tau = (a_1\ a_2\ a_3 \cdots)(b_1\ b_2 \cdots) \cdots . \quad \cdots\cdots (*)$$

Then, since $n \geq 4$, $\sigma \in G$, $a_1 \mapsto a_1$, $a_2 \mapsto a_2$, $a_3 \mapsto a_3$, exists. And by prop 10, we have $\tau_1 := \sigma\tau\sigma^{-1} = (a_1\ a_2\ \sigma(a_3) \cdots)(\sigma(b_1)\ \sigma(b_2) \cdots)$ with $\tau_1 \neq \tau_2$ and $\tau_1(a_1) = \tau_2(a_2)$, a contradiction.

KOKUYO LOOSE-LEAF J-836BT 6 mm ruled×36 lines

No.

Date

Therefore, every nontrivial element τ in H, since $n \geq 6$ and (*) does not hold, τ has the has the form of cycle decomposition, $(a_1\ a_2)(a_3\ a_4)(a_5\ a_6)\cdots$. Define $\sigma = (a_1\ a_2)(a_3\ a_5)$ then, $\tau_1 := \sigma\tau\sigma^{-1} = (a_1\ a_2)(a_3\ a_6)(a_5\ a_4)\cdots$. with $\tau \neq \tau_1$ and $\tau(a_1) = \tau_1(a_1)$, a contradiction.

Therefore, A_n does not possess nontrivial normal subgroup, A_n is simple for $n \geq 5$.

Prop 1. If $G_1, \cdots, G_n$ are groups, their direct product is a group of order $|G_1| \cdots |G_n|$.

Proof) Obvious.

Prop 2. Let $G_1, \cdots, G_n$ be groups and let $G = G_1 \times \cdots \times G_n$ be their direct product.

(1) For each fixed i the set of elements of G which have the identity of G_j in the j^{th} position for all $j \neq i$ and arbitrary elements of G_i in position i is a subgroup of G isomorphic to G_i. If we identify G_i with this subgroup, then $G_i \trianglelefteq G$ and

$G/G_i \cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n$.

(2) For each fixed i define $\pi_i : G \to G_i$ by $\pi_i((g_1, \cdots, g_n)) = g_i$.

Then π_i is a surjective homomorphism with $\ker \pi_i \cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n$.

(3) Under the identifications in part (1), if $x \in G_i$ and $y \in G_j$ for some $i \neq j$, then

$xy = yx$.

Proof)

Let $f : g_i \mapsto (id, \cdots, id, g_i, id, \cdots, id)$. Then clearly f is isomorphism from G_i onto the subgroup of G.

Next, we verify $G_i \trianglelefteq G$.

$\forall g \in G_i$, $\forall (g_1, \cdots, g_n) \in G$

$(g_1, \cdots, g_n) \cdot (id, \cdots id, g, id, \cdots, id)(g_1^{-1}, \cdots, g_n^{-1}) = (id, \cdots, id, g_i \cdot g \cdot g_i^{-1}, id, \cdots id)$

thus, $G_i \trianglelefteq G$.

Finally, we verify, $G/G_i \cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n$

KOKUYO LOOSE-LEAF ノ-836B 6 mm ruled×36 lines

Let $\varphi : G \to G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n ; (g_1, \cdots, g_n) \mapsto (g_1, \cdots, g_{i-1}, g_{i+1}, \cdots, g_n)$.

Then clearly φ is homeomorphism and surjective, moreover $\ker \varphi = G_i$ holds.

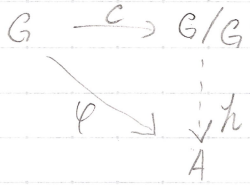
Thus, $G/G_i \approx G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n$.

(2) Since, $\ker \pi_i = \{ (g_1, \cdots, g_{i-1}, id, g_{i+1}, \cdots, g_n) \in G \}$ holds,

$\ker \pi_i \approx G/G_i \approx G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n$.

(3) Obvious.

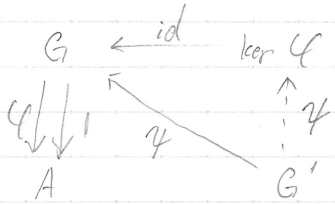
(5) If $\varphi(g_1) = \varphi(g_2)$ i.e. $G' \leq \ker\varphi$ holds, TFTDC,



$c : g \longmapsto g \cdot G'$

$h : gG' \longmapsto \varphi(g)$ independent of choice.

Now, for $id : G' \to G$, $\varphi \circ id\,(g_1^{-1} \cdot g_2^{-1} \cdot g_1 \cdot g_2) = 1$ holds, TFTDC,



Hence, $G' \leq \ker\varphi$ holds.

Prop 8. Let H and K be subgroups of the group G. The number of distinct ways of writing each element of the set HK in the form hk, for some $h \in H$ and $k \in K$ is $|H \cap K|$.

In paticular, if $H \cap K = id$, then each element of HK can be written uniquely as a product hk, for some $h \in H$ and $k \in K$.

Proof). On $H \times K$ define relation "$\sim$", $(h_1, k_1) \sim (h_2, k_2)$ if $h_1 \cdot k_1 = h_2 \cdot k_2$ then $\sim$ is equivalent relation. Since, $\forall x \in H \cap K$, $(h_1, k_1) \sim (h_1 x, x^{-1} k_1)$ holds, then every equivalence class possesses elements more than or equals to $|H \cap K|$. Thus, the number of equivalence class is less than $\frac{|H \times K|}{|H \cap K|}$. And now, $|H \cdot K| = \frac{|H| \cdot |K|}{|H \cap K|}$, $|H \times K / \sim| = \frac{|H \times K|}{|H \cap K|}$ holds. Then, if there exists some equivalence class which has order properly more than $|H \cap K|$. Then, the number of equivalence class is properly less than $\frac{|H \times K|}{|H \cap K|}$, a contradiction.

KOKUYO LOOSE-LEAF ノ-836BT 6 mm ruled × 36 lines

Hence, every equivalence class possesses elements $|H \cap K|$.

Thm 9. Suppose G is a group with subgroups H and K such that,

(1) H and K are normal in G, and

(2) $H \cap K = id$.

Then, $HK \simeq H \times K$.

Proof) By previous theorem, the function $\varphi : HK \to H \times K \; ; x \mapsto \langle h, k \rangle$ with $x = hk$.

is determined independent of choice. We verify φ is isomorphism, it is clearly φ is bijective

thus, verify φ is homorphism.

Since, $H \trianglelefteq G$, for h, k $k \cdot h \cdot k^{-1} \in H$ moreover, $h^{-1} \cdot k \cdot h \cdot k^{-1} \in H$ holds,

similaly, since $K \trianglelefteq G$, $h^{-1} \cdot k \cdot h \cdot k^{-1} \in K$ holds. Thus, $h^{-1} k h k^{-1} = id$, $kh = hk$.

For, $h_1, h_2 \in H$, $k_1, k_2 \in K$.

$$\varphi(h_1 \cdot k_1) \cdot \varphi(h_2 \cdot k_2) = \langle h_1, k_1 \rangle \cdot \langle h_2, k_2 \rangle$$

$$= \langle h_1 h_2, k_1 \cdot k_2 \rangle$$

$$= \varphi(h_1 \cdot h_2, k_1 k_2) \quad \text{thus, } \varphi \text{ is homomorphism.}$$

Hence, $HK \simeq H \times K$

Thm 10. Let H and K be groups and let φ be a homomorphism from K into $Aut(H)$. Let $\cdot$ denote the left action of K on H determined by φ. Let G be the set of ordered pairs (h, k) with $h \in H$ and $k \in K$ and define the following multiplication on $(h_1, k_1) \cdot (h_2, k_2) = (h_1 \cdot k_1 \cdot h_2, k_1 k_2)$

Prop 7 Let G be a group, let $x, y \in G$ and let $H \leq G$. Then

(1) $xy = yx[x,y]$ in particular, $xy = yx$ iff $[x,y] = 1$.

(2) $H \trianglelefteq G$ iff $[H,G] \leq H$.

(3) G' is characteristic subgroup of G and G/G' is Abelian.

(4) G/G' is the largest Abelian quotient of G in the sense that if $H \trianglelefteq G$ and G/H is Abelian, then $G' \leq H$. Conversely, if $G' \leq H$, then $H \trianglelefteq G$ and G/H is Abelian.

(5) If $\varphi : G \to A$ is any homomorphism of G into an Abelian group A, then φ factors through G'.

Proof)

(1) Obvious.

(2)

($\Rightarrow$) For arbitrary $h_1, h_2 \in H, g \in G$ verify $h_2(h_1^{-1} g^{-1} h_1 \cdot g) h_2^{-1} \in H$.

Since, $H \trianglelefteq G$, $g^{-1} \cdot h_1 \cdot g \in H$ thus, $[H,G] \trianglelefteq H$

($\Leftarrow$) $\forall h \in H, \forall g \in G$ since, $[H,G] \trianglelefteq H$,

$$h(h^{-1} \cdot g \cdot h \cdot g^{-1}) h^{-1} \in H.$$

$$g h \cdot g^{-1} h^{-1} \in H$$

$$g h g^{-1} \in H$$

Hence, $H \trianglelefteq G$ holds.

(3) Let σ be an automorphism of G.

KOKUYO LOOSE-LEAF J-836BT 6 mm ruled×36 lines

$\sigma[x,y] = \sigma(x^{-1}\cdot y^{-1}\cdot x\cdot y)$

$= \sigma(x)^{-1}\cdot\sigma(y)^{-1}\cdot\sigma(x)\cdot\sigma(y) \in [G,G]$ for every $x,y\in G$.

Thus, G' is characteristic subgroup of G.

Nest we show G/G' is Abelian.

First, we verify G/G' form the group i.e. G' is normal.

$\forall g\in G, \forall g'\in G'.\quad g\cdot g'\cdot g^{-1} = g'\cdot(g^{-1}\cdot g\cdot g'\cdot g^{-1})\in G'.$

Thus, G' is normal, G/G' form the group.

For $g_1,g_2\in G$, $g\in G'$, we verify $(g_1\cdot g_2)\cdot g \in (g_2\cdot g_1)\,G'$.

Now, $g_1^{-1}\cdot g_2^{-1}\cdot g_1\cdot g_2\in G'$ and $g\in G'$ thus, $(g_1^{-1}\,g_2^{-1}\cdot g_1\,g_2)\,g\in G'$ moreover,

$g_1\cdot g_2\cdot g \in g_1\cdot g_2\,G'$. Hence, $(g_1\cdot g_2)G' = (g_2\cdot g_1)\,G'$ holds, G/G' is Abelian.

(4)

($\Rightarrow$) Since, $(xH)(yH) = (yH)(xH)$ holds,

$id\,H = (xH)^{-1}\cdot(yH)^{-1}\cdot(xH)(yH)$

$= [x,y]H$. Thus, $G'\le H$.

($\Leftarrow$) If $G'\le H$. Since G/G' is Abelian, every subgroup of G/G' is normal,

$H/G' \trianglelefteq G/G'$ holds moreover by Lattice Isomorphism Theorem $H\trianglelefteq G$ and by Third Isomorphism Theorem, $G/H \approx (G/G')/(H/G')$.

Since, G/G' is Abelian, G/H is also Abelian.

(1) This multiplication makes G into a group of order $|G| = |H| \cdot |K|$.

(2) The sets $\{(h, id) ; h \in H\}$ and $\{(id, k) ; k \in K\}$ are subgroups of G and the maps $h \mapsto (h, id)$ for $h \in H$ and $k \mapsto (id, k)$ for $k \in K$ are isomorphisms of these subsubgroups with the groups H and K respectively:

$$H \simeq \{(h, id) ; h \in H\} \text{ and } K \simeq \{(id, k) ; k \in K\}.$$

Identifying H and K with their isomorphic copies in G described in (2) we have

(3) $H \trianglelefteq G$

(4) $H \cap K = id$

(5) for all $h \in H$ and $k \in K$, $khk^{-1} = k \cdot h$.

Proof)

(i) First, we verify G form the group.

(i) $(id, id) \in G$ is an identity.

$(h, k) \cdot (id, id) = (h, k)$, $(id, id)(h, k) = (h, k)$ holds.

(ii) For $(h, k) \in G$, $(h^{-1}, k^{-1}) \in G$ is an inverse elements.

$(h, k) \cdot (h^{-1}, k^{-1}) = id$, $(h^{-1}, k^{-1})(h, k) = id$ holds.

(iii) For (h_1, k_1), (h_2, k_2) and $(h_3, k_3) \in G$

$$\begin{aligned}((h_1, k_1) \cdot (h_2, k_2)) \cdot (h_3, k_3) &= (h_1 k_1 \cdot h_2, k_1 \cdot k_2)(h_3, k_3) \\ &= (h_1 \cdot (k_1 \cdot h_2) \cdot (k_1 \cdot k_2) \cdot h_3, k_1 k_2 k_3) \\ &= (h_1 \cdot \varphi(k_1)(h_2) \cdot \varphi(k_1 \cdot k_2)(h_3), k_1 k_2 k_3)\end{aligned}$$

KOKUYO LOOSE-LEAF A-836BT 6 mm ruled x36 lines

$= (h_1 \cdot \varphi(k_1)(h_2) \cdot \varphi(k_1)(\varphi(k_2)(h_3)) \; k_1 k_2 k_3)$

$= (h_1 \cdot k_1 \cdot (h_2 \cdot k_2 \cdot h_3), k_1 k_2 k_3)$

$= (h_1, k_1)((h_2, k_2)(h_2, k_3))$.

(2) $\forall h_1, h_2 \in H$

$(h_1, id) \cdot (h_2, id)^{-1} = (h_1, id) \cdot (h_2^{-1}, id) = (h_1 \cdot h_2^{-1}, id) \in H$

$\forall k_1, k_2 \in K$

$(id, k_1) \cdot (id, k_2)^{-1} = (id, k_1) \cdot (id, k_2^{-1}) = (id, k_1 k_2^{-1}) \in K$.

Thus, H and K are subgroup.

Let, $\eta : h \mapsto (h, id)$. $\varepsilon : k \mapsto (id, k)$.

for all $h_1, h_2 \in H$, $\eta(h_1) \cdot \eta(h_2) = (h_1, id) \cdot (h_2, id) = (h_1 \cdot h_2, id) = \eta(h_1 h_2)$

for all $k_1, k_2 \in K$, $\varepsilon(k_1) \cdot \varepsilon(k_2) = (id, k_1)(id, k_2) = \varepsilon(k_1 \cdot k_2)$ holds,

η, ε are isomorphism.

(3) $H \trianglelefteq G$

$\forall h \in H$, $(h_1, k_1) \in G$,

$(h_1, k_1) \cdot h \cdot (h_1, k_1)^{-1} = (h_1 \cdot h, k_1)(h_1^{-1}, k_1^{-1})$

$= (-, k_1 \cdot k_1^{-1}) \in H$ Thus, H is normal.

(4) For arbitrary $x \in H \cap K$, $(h_1, k_1), (h_2, k_2) \in G$,

$(h_1, k_1) \cdot (h_2, k_2) = (h_1, k_1 \cdot x^{-1})(x \cdot h_2, x k_2)$ holds,

By (1), exists bijection $H \times K$ onto G, every elements in G has unique from (u, v) then

$x = id$ i.e. $H \cap K = id$.

(5) $\forall h, k$

$$(id, k)(h, id)(id, k)^{-1} = (khk^{-1}, k)(id, k^{-1})$$

$$= (khk^{-1}, id).$$

Thus, $khk^{-1} = k \cdot h$ holds.

Prop 11 Let H and K be groups and let $\varphi : K \to Aut(H)$ be a homomorphism.

Then the following are equivalent:

(1) the identity map between $H \rtimes K$ and $H \times K$ is a group homomorphism.

(2) φ is the trivial homomorphism from K into $Aut(H)$

(3) $K \trianglelefteq H \rtimes K$.

Proof)

(1) $\Rightarrow$ (2)

By assumption for $(h_1, k_1), (h_2, k_2)$, $(h_1 \cdot k_1 h_2 k_1^{-1}, k_1 k_2) = (h_1 h_2, k_1 k_2)$ holds.

Thus $k_1 \cdot h_2 = h_2$ holds for all k_1 and h_2, then φ is trivial.

(2) $\Rightarrow$ (1)

$\forall k \in K$, $(h, k) \in H \rtimes K$,

$$((h, k) \circ (id, k')) \circ (h, k)^{-1} = (h, k \cdot k') \circ (h^{-1}, k^{-1})$$

$$= (id, k k' k^{-1}) \quad (\because \varphi \text{ is trivial})$$

$$\in K$$

Therefore, $K \trianglelefteq H \rtimes K$

KOKUYO LOOSE-LEAF ノ-836BT 6 mm ruled×30 lines

(3) $\Rightarrow$ (1)

First we verify for arbitrary h, k, $[h,k] \in K$ holds.

Since, $K \trianglelefteq H \rtimes K$ holds, $[h,k] \in K$ is clear.

And since, $(h^{-1}, id)\circ(id, k)\circ(h, id)\circ(id, k) = (h^{-1}, k^{-1})\circ(h, k) \in H$.

Then, $[h,k] \in H \cap K$ moreover by previous theorem, $[h,k] = id$ and $k \cdot h = khk^{-1}$ holds, the action of K on H is trivial thus the identity map is isomorphism.

Thm 12.

Suppose G is a group with subgroups H and K such that

(1) $H \trianglelefteq G$, and

(2) $H \cap K = id$.

Let $\varphi : K \to Aut(H)$ be the homomorphism defined by mapping $k \in K$ to the automorphism of left conjugation by k on H. Then $HK \cong H \rtimes K$. In particular, if $G = HK$ with H and K satisfying (1) and (2), then G is the semidirect product of H and K.

Proof)

By thm 8, every element u in HK there exists unique pair (h,k) such that $u = hk$ thus we can define the function $f : hk \mapsto (h,k)$ independent of choice.

For $h_1k_1, h_2k_2 \in HK$, $f((h_1k_1)(h_2k_2)) = f(h_1k_1h_2k_2) = (h_1k_1h_2k_1^{-1}, k_1k_2)$

$= (h_1, k_1)\cdot(h_2, k_2)$ thus f is isomorphism, $HK \cong H \rtimes K$.

Thm1 Let p be a prime and let P be a group of order p^α, $\alpha \geq 1$. Then

(1) The center of P is nontrivial i.e. $Z(P) \neq id$

(2) If H is nontrivial normal subgroup of P then $H \cap Z(P) \neq id$.

(3) If H is a normal subgroup of P then H contains a subgroup of order p^b that is normal in P for each divisor p^b of $|H|$. In paticular, P has a normal subgroup of order p^b for every $b \in \{0, \cdots, a\}$.

(4) If $H < P$ then $H < N_P(H)$.

(5) Every maximal subgroup of P is of index p and is normal in P.

Proof)

(1) See Thm 8 of Sec 4.3

(2) Let H be a non-trivial normal subgroup of P, then H has the form of the union of equivalent class $H = \bigcup_{1 \leq i \leq n} E_i$, E_i is conjugacy class of P and let for $1 \leq i \leq s$, E_i is singleton, for $s+1 \leq i \leq n$, E_i is not singleton and every E_i is pairwise distincts. Then clearly,

$$\begin{aligned} |H| &= \sum_{1 \leq i \leq n} |E_i| \\ &= \sum_{1 \leq i \leq s} |E_i| + \sum_{s+1 \leq i \leq n} |E_i| \\ &= |H \cap Z(P)| + \sum_{s+1 \leq i \leq n} \frac{|P|}{|C_P(a_i)|}, \text{ pick an } a_i \text{ from } E_i. \end{aligned}$$

Since, $|H|$ and every $\frac{|P|}{|C_P(a_i)|}$ divided by p, $p \mid |H \cap Z(P)|$ and $|H \cap Z(P)| \neq \{\}$ thus, $H \cap Z(P) \neq id$.

(3) We prove by induction on a.

If $a=1$ or $H=id$, it is clearly holds.

Let $a>1$ and $H \neq id$. By (2), $p \mid |H \cap Z(P)|$ thus by Cauchy's theorem, $H \cap Z(P)$ has subgroup Z_1 of order p, we assert Z_1 is normal in P. Since $H \trianglelefteq P$ implies $H/Z_1 \trianglelefteq P/Z_1$ and $|P/Z_1| = p^{a-1}$, by assumption, H/Z_1 possesses subgroup $K/Z_1 (\trianglelefteq P/Z_1)$ of order p^b. for every $b \leq a-1$. Then by Lattice Isomorphism theorem, H possesses subgroup $K (\trianglelefteq P)$ of order p^b for every $1 \leq b \leq a$. And clearly H possesses the normal subgroup of order 1. This complete the proof.

(4) We prove by induction on a.

If $a=1$, then $H < P$ implies $H = id$ thus $H < N_P(H)$ holds.

Let $a>1$.

If $Z(P) \not\leq H$ holds, then $\langle H, Z(P) \rangle \neq H, Z(P)$ moreover, $H \lneq \langle H, Z(P) \rangle \leq N_P(H)$ holds. thus $H \lneq N_P(H)$.

if $Z(P) \trianglelefteq H$ holds, $H/Z(P)$ form the group.

Hereafter for $Z(P) \trianglelefteq G$, $\bar{G} := G/Z(P)$.

By assumption, $\bar{H} \lneq N_{\bar{P}}(\bar{H})$ holds. And by $N_{\bar{P}}(\bar{H}) \leq \overline{N_P(H)}$, $\bar{H} \lneq \overline{N_P(H)}$ thus, $H \lneq N_P(H)$ holds. This complete the proof.

(5) Let M be a maximal normal subgroup of P. Then by (4) $M < N_P(M)$ holds. By maximality of M, $N_P(M) = P$ thus, $M \trianglelefteq P$ holds.

If $|M/P| > p$, M/P possesses a subgroup of P i.e. there exists subgroup of P which is superset of M a contradiction.

Thus, $|M/P| = p$, $|M| = p^{a-1}$.

Prop2. Let p be a prime and let P be a group of order p^a. Then P is nilpotent of nilpotence class at most $a-1$.

Proof) If $Z_i(P) \neq P$, by Thm 1(1), $p \mid |Z(P/Z_i(P))|$ thus, $|Z_{i+1}/Z_i| = |Z(P/Z_i(P))| \geq p$ moreover, $|Z_{i+1}| \geq p|Z_i|$.

Thus, whenever $Z_{a-1}(P) \neq P$, $|Z_a| \geq p^a$ holds thus $Z_a = P$.

Hence, P is nilpotent of class $\leq a$.

If the nilpotent class is a, this force $|Z_i(P)| = p^i$ for every i.

Thus, $|P/Z_{a-2}| = p^2$ by Sec 4.3 Cor 9, P/Z_{a-2} is an Abelian thus $P/Z_{a-2} = Z(P/Z_{a-2})$ thus $Z_{a-1} = P$, a contradiction.

Thus the nilpotent class is at most $a-1$.

KOKUYO LOOSE LEAF

Prop 1 Let R be a ring. Then

(1) $0a = a0 = 0$ for all $a \in R$

(2) $(-a)b = a(-b) = -(ab)$ for all $a, b \in R$

(3) $(-a)(-b) = ab$ for all $a, b \in R$

(4) if R has an identity 1, then the identity is unique and $-a = (-1)a$.

Proof).

(1) Since $(0+0)a = 0a + 0a$ holds, clearly $0 = 0a$ and the same way $0 = a0$.

(2) Since $(a+(-a))b = ab + (-a)b$ holds, $-(ab) = (-a)b$ and the same way, $-(ab) = a(-b)$.

(3) by (2) $(-a)(-b) = -(-(ab)) = ab$.

(4) Let e be an identity of R,

then $1 = 1 \cdot e = e$. thus the identity is unique.

Since $a + (-1)a = (1 + (-1))a = 0$ holds, clearly $-a = (-1)a$.

Prop 2 Assume a, b and c are element of any ring with a not a zero divisor. If $ab = ac$, then either $a = 0$ or $b = c$. In particular, if a, b, c are any elements in an integral domain and $ab = ac$, then either $a = 0$ or $b = c$.

Proof)

By $ab = ac$, $a(b-c) = 0$ holds.

If a is non-zero element, $b - c = 0$ thus, $a = 0$ or $b - c = 0$.

KOKUYO LOOSE-LEAF ノ-836BT 6 mm rule×36 lines

Cor 3. Any finite integral domain is a field.

Proof) Let a be a non-zero element then $aR \subset R$ holds.

By pervious theorem, $b \neq b'$ implies $ab = ab'$ and since R is finite, $aR = R$

Hence, there exists some b such that $ab = 1$ thus, R form the field.

Prop4. Let R be an integral domain and let $p(x)$, $q(x)$ be non-zero elements of $R[x]$.

Then,

(1) degree $p(x) \cdot q(x)$ = degree $p(x)$ + degree $q(x)$,

(2) the units of $R[x]$ are just the unit of R,

(3) $R[x]$ is an integral domain.

Proof) Let $a_n \cdot x^n$ and $b_m \cdot x^m$ be leading terms of $p(x)$ and $q(x)$, then the leading term of $p(x) \cdot q(x)$ is $a_n \cdot b_m \cdot x^{n+m}$ thus (1) holds and moreover, since R is integral domain, $R[x]$ is also an integral domain.

(2) If $p(x)$ is a unit of $R[x]$ then for some $q(x)$, $p(x) \cdot q(x) = 1$ holds.

This show that degrees of $p(x)$ and $q(x)$ are 0, thus $p(x)$ is also the unit of R.

Prop5. Let R and S be rings and let $\varphi : R \to S$ be a homomorphism.

(1) The image of φ is a subring of S.

(2) The kernel of φ is a subring of R. Futhermore, if $a \in \ker \varphi$ ther ra and $ar \in \ker \varphi$ for every $r \in R$ i.e. $\ker \varphi$ is closed under multiplication by elements from R.

Proof).

(1) Clearly $0 \in \mathrm{Im}\,\varphi$. Let $s_1, s_2 \in \mathrm{Im}\,\varphi$ then there exists $r_1, r_2 \in R$ such that $\varphi r_1 = s_1$ and $\varphi r_2 = s_2$ hold. Then, $\varphi(r_1 - r_2) = s_1 - s_2$ and $\varphi(r_1 \cdot r_2) = s_1 \cdot s_2$ hold. This assert $s_1 - s_2$, $s_1 \cdot s_2 \in \mathrm{Im}\,\varphi$. Thus, $\mathrm{Im}\,\varphi$ is closed under subtraction and multiplication.

(2) Clearly $0 \in \ker\varphi$. Let $r_1, r_2 \in \ker\varphi$ then $\varphi r_1 = \varphi r_2 = 0$ hold. Thus, $\varphi(r_1 - r_2) = 0$ and $\varphi(r_1 \cdot r_2) = 0$. Thus, $\ker\varphi$ is closed under subtraction and multiplication. And the same ways, for arbitrary $r \in R$ and $\alpha \in \ker\varphi$ we have $\varphi(r\alpha) = 0$ and $\varphi(\alpha r) = 0$ thus, $r\alpha, \alpha r \in \ker\varphi$.

Prop 6 Let R be a ring and let I be an ideal of R. Then the additive quotient group R/I is a ring under the binary operations,

$$(r+I) + (s+I) = (r+s) + I \quad \text{and} \quad (r+I) \times (s+I) = (r \times s) + I.$$

for all $r, s \in R$. Conversely, if I is any subgroup of R such that the above operations are well-defined, then I is an ideal of R.

Proof) Suppose, I is ideal, we verify the operations are well-defined. Let $r, r', s, s' \in R$ such that $r + I = r' + I$ and $s + I = s' + I$ hold. To show the addition is well-defined, it is enough to verify $r + s \in (r' + s') + I$ holds. However, since R is Abelian group it is clearly holds. Next we verify the multiplication is well-defined, $(r \cdot s) \in (r' + s') + I$ holds. Let $\alpha, \beta \in I$ such that $r = r' + \alpha$ and $s = s' + \beta$ then,

$$rs = (r' + \alpha) \cdot (s' + \beta) = r's' + \alpha s' + r'\beta + \alpha\beta \in r's' + I \text{ holds.}$$

KOKUYO LOOSE-LEAF ノ-836BT 6 mm ruled×36 lines

Hence, the multiplication is well-defined.

Next, suppose the addition and the multiplication on R/I are well-defined.

Since, I is a subgroup of R, it is enough to verify I is closed under multiplication and $rI, Ir \subset I$ hold for all $r \in R$.

By, $(0+I)\cdot(0+I) = I$, clearly $xy \in I$ for all $x, y \in I$.

And by $(r+I)\cdot(0+I) = I$, $r \cdot i \in I$ for all $r \in R$ and $i \in I$. Similaly $Ir \subset I$.

Hence, I form the ideal of R.

Thm7.

(1) The First Isomorphism Theorem for Rings.

If $\varphi : R \to S$ is a homomorphism of rings, then the kernel of φ is an ideal of R, the image of φ is a subring of S and $R/\ker\varphi$ is isomorphic as a ring to $\varphi(R)$.

(2) If I is any ideal of R, then the map $R \to R/I$ defined by $r \mapsto r+I$ is a surjective ring homomorphism with kernel I this homomorphism is called the natural projection of R onto R/I. Thus every ideal is the kernel of a ring homomorphism and vice-versa.

Proof)

(1) By prop 5 (2) it is clearly the $\ker\varphi$ is an ideal of R and by prop 5 (1) image of φ is a subring of S.

Next, we verify $R/\ker\varphi \simeq \varphi(R)$

Now for $a, b \in R$, $a + \ker\varphi = b + \ker\varphi$, $-a + b \in \ker\varphi$ holds. Thus, $\varphi(b) - \varphi(a) = 0$ moreover $\varphi(a) = \varphi(b)$ holds. Hence the function φ' as follows well-defined

$$\varphi' : R/\ker\varphi \to \varphi(R) \; ; \; r + \ker\varphi \mapsto \varphi(r).$$

Then, clearly φ' is isomorphism, $R/\ker\varphi \approx \varphi(R)$ holds.

(2) Since $\ker\varphi = I$ holds by (1) clearly holds.

Thm8. Let R be a ring.

(1) The secound Isomorphism Theorem for Rings.

Let A be a subring and let B be an ideal of R. Then $A+B = \{a+b ; a \in A, b \in B\}$ is a subring of R, $A \cap B$ is an ideal of A and $(A+B)/B \approx A/(A \cap B)$.

(2) The Third Isomorphism Theorem for Rings.

Let I and $\mathfrak{J}$ be ideals of R with $I \subseteq \mathfrak{J}$. Then $\mathfrak{J}/I$ is an ideal of R/I and $(R/I)/(\mathfrak{J}/I) \approx R/\mathfrak{J}$.

(3) The Flourth or Lattice Isomorphism Theorem for Rings.

Let I be an ideal of R. The correspondence $A \leftrightarrow A/I$ is an inclusion preserving bijection between the set of subrings of A of R that contain I and the set of subrings of R/I.

Futhermore, A is an ideal of R iff A/I is an ideal of R/I.

Proof.) For arbitrary $a, a' \in A$, $b, b' \in B$.

Since $(a+b) - (a'+b') = (a-a') + (b-b')$ holds,

KOKUYO LOOSE-LEAF 7-R8BT 6mm ruled ×36 Lines

$A+B$ is closed under subtraction.

And since $(a+b)\cdot(a'+b') = aa'+(ab'+ba'+bb') \in A+B$, $A+B$ is closed under multiplication.

Next, we verify $A\cap B$ is an ideal of A.

By previous fact, $A\cap B$ is a subring of A.

For $a, a' \in A$, $b \in B$, $a'(a+b) = a'\cdot a + a'b \in A+B$, $(a+b)a' \in A+B$ hold.

$A\cap B$ is an ideal of A.

Next, we verify $(A+B)/B \simeq A/(A\cap B)$.

Now, we assert $a+b = a'+b'$ implies $a-a' \in A\cap B$.

Let $\varphi : A+B \longrightarrow A/(A\cap B)$; $a+b \mapsto a+A\cap B$.

We verify $\ker\varphi = B$.

$\forall b \in B$, $\varphi(b) = 0+A\cap B$ thus, $B \subset \ker\varphi$.

$\forall b \in \ker\varphi$ $b \in A\cap B \subset B$

Hence, $\ker\varphi = B$ thus, $(A+B)/B \simeq A/(A\cap B)$

(2) Let $\varphi : R/I \longrightarrow R/\mathfrak{J}$; $r+I \mapsto r+\mathfrak{J}$.

Clearly φ is ring homomorphism, we assert $\ker\varphi = \mathfrak{J}/I$.

$\forall j+I \in \mathfrak{J}+I$, $\varphi(j+I) = j+\mathfrak{J} \in \mathfrak{J}$ thus, $\mathfrak{J}/I \subset \ker\varphi$.

$\forall j+I \in \ker\varphi$, $j \in \mathfrak{J}$ thus, $\ker\varphi \subset \mathfrak{J}/I$.

Therefore, $(R/I)/(\mathfrak{J}/I) \simeq R/\mathfrak{J}$.

(3) It is enough to verify $A/I = B/I$ implies $A = B$ and $A = B$ implies $A/I = B/I$.

Suppose, $A/I = B/I$.

$\forall a \in A \ \exists b \in B.\ a+I = b+I$, $a-b \in I \subset B$ thus, $a \in B$.

Similarly $\forall b \in B,\ b \in A$. Hence $A = B$ holds.

Suppose $A = B$.

$\forall a+I \in A+I$ since $a \in B$, $a+I \in B/I$. Similarly $\forall b+I \in B+I$, $b+I \in A/I$.

Hence $A/I = B/I$.

Therefore A and A/I has one to one correspondence.

Prop 9. Let I be an ideal of R.

(1) $I = R$ iff I contains a unit.

(2) Assume R is commutative. Then R is a field iff its only ideals are 0 and R.

Proof.)

(1) ($\Rightarrow$) Obvious.

($\Leftarrow$) Let u be a unit of I with s such that $u \cdot s = s u = 1$ then for $r \in R$,

$r = r(u \cdot s) = (ru) \cdot s \in I$. Hence $I = R$.

(2) ($\Rightarrow$) Let I be an ideal. Suppose $\exists\, i,\ i \in I \setminus \{0\}$. Since R is a division ring

there exists $j \in R$ such that $ij = 1$ moreover, since I is an ideal $ij \in I$.

Hence, $1 \in I$ and by (1), $R = I$.

KOKUYO LOOSE-LEAF J-836BT 6 mm ruled×36 lines

($\Leftarrow$) If only ideals of R are 0 and R, then let $\forall u \in R$ with $u \neq 0$, then $(u) = R = uR$.

Thus, $\exists v \in R$, $uv = 1 = vu$ holds. Then, u is a unit, R is a field.

Cor 10. If R is a field then any nonzero ring homomorphism from R into another ring is an injection.

Proof.) Let $\varphi : R \to S$ be any nonzero ring homomorphism where R is a field and S is a ring. Since $\exists r \in R$ with $\varphi(r) \neq 0$, $\ker \varphi \subsetneq R$.

Since $\ker \varphi$ is an ideal by prop 9 $1 \ker \varphi = 0$.

Thus for $r, r' \in R$ if $\varphi(r) = \varphi(r')$ holds, $r = r'$ holds.

Prop 11. In a ring with identity every proper ideal is contained in a maximal ideal.

Proof.) Let R be a ring with identity and let I be a proper ideal of R. Let S be the collection of all proper ideals of R which include in I. Then clearly $S \neq \{\}$ and S is partically ordered by inclusion relation.

For a chain $\mathcal{C}$ in S, define $\mathcal{J} := \bigcup_{A \in \mathcal{C}} A$. We prove that $\mathcal{J} \in S$.

First we show that $\mathcal{J}$ is an ideal of R.

Clearly, $\mathcal{J} \neq \{\}$. For all $a, b \in \mathcal{J}$ there exists $A, B \in \mathcal{C}$ such that $a \in A$, $b \in B$.

Since $A \subset B$ or $B \subset A$, $a - b \in B$ or $a - b \in A$ respectively. In either way, $a - b \in \mathcal{J}$, similarly $ab \in \mathcal{J}$.

Also, for all $r \in R$ and $x \in \mathcal{J}$, since each $A \in \mathcal{C}$ is an ideal, $rx, xr \in \mathcal{J}$.

Next, suppose $\mathcal{J}$ is not a proper ideal, $\mathcal{J} = R$ holds.

Then, $1 \in \mathcal{J}$ so, for some $A \in \mathcal{C}$, $1 \in A$ holds. Thus by prop 9(1). $A = R$ this contradicts that A is proper ideal of R. Therefore $\mathcal{J} \in S$.

Therefore every chain in S is upper bounded thus by Zorn's lemma S has a maximal proper ideal of R including I.

Prop12 Assume R is commutative. The ideal M is a maximal ideal iff the quotient ring R/M is a field.

Proof) Prop 9. (2) assert R/M is a field iff an ideal of R/M is M/M or R/M. And by the Fourth isomorphism theorem, an ideal of R and an ideal of R/M has the correspondence. This prove this proposition.

Prop13. Assume R is commutative. Then the ideal P is a prime ideal in R iff the quotient ring R/P is an integral domain.

Proof) Note that since R is a commutative ring with identity 1, the quotient ring R/P is clearly a commutative ring with identity $1+P$. Thus, we have to show that P is a prime ideal iff R/P has no zero-divisors.

$\Leftrightarrow$) Let P be a prime ideal in R and R/P has zero divisor $r+P$. Then for some $s+P \in R/P$, $s+P \neq 0+P$ and $(s+P)(r+P) = 0+P$ hold.

Then, by $(s+P)(r+P) = 0+P$, $sr \in P$ since P is prime ideal, r or $s \in P$.

However, this contradicts $r+P \neq 0+P$ or $s+P \neq 0+P$. Thus R/P has no zero divisor.

KOKUYO LOOSE-LEAF ノ-836RT 6 mm ruled × 36 lines

($\Leftarrow$) Let $ab \in R$. If $ab \in P$ then, $(a+P)(b+P) = 0+P$. Since R/P has no zero-divisor, $a+P = 0+P$ or $b+P = 0+P$. This show $a \in P$ or $b \in P$.

Cor 14. Assume R is commutative. Every maximal ideal of R is a prime ideal.

Proof) Let M be a maximal ideal. By prop 12, R/M is a field. Since every field is an integral domain, by prop 13, M is a prime ideal.

Thm 15. Let R be a commutative ring. Let D be any nonempty subset of R that does not contain 0, does not contain any zero divisors and is closed under multiplication. Then there is a commutative ring Q with 1 such that Q contains R as a subring and every element of D is a unit in Q. The ring Q has the following additional properties.

(1) every element of Q is of the form rd^{-1} for some $r \in R$ and $d \in D$. In patticular, if $D = R \setminus \{0\}$ then Q is a field.

(2) The ring Q is the "smallest" ring containg R in which all elements of D become unit.

Proof) Let $\mathcal{F} := \{(r,d) ; r \in R, d \in D\}$ and define the relation $\sim$ on $\mathcal{F}$ by $(r,d) \sim (s,e)$ if $re = sd$. We verify $\sim$ is an equivalent relation.

Since R is commutative ring, clearly $(r,d) \sim (r,d)$ and $(r,d) \sim (s,e)$ implies $(s,e) \sim (r,d)$. Suppose $(r,d) \sim (s,e)$ and $(s,e) \sim (t,f)$, then $re - sd = 0$ and $sf = te$ so, $(re - sd)f = 0$, $ref - sdf = 0$ moreover,

$(rf - td)e = 0$ since $e \in D$, $rf - td = 0$, $rf = td$. Hence $(r, d) \sim (t, f)$ holds.

Therefore, $\sim$ is an equivalent relation.

Hereafter the equivalent class of (r, d) by $\frac{r}{d}$. Let Q be the set of equivalent class under $\sim$. Note that $\frac{r}{d} = \frac{re}{de}$ for all $e \in D$.

Define the addition and multiplication on Q by

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \quad \text{and} \quad \frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}.$$

First we verify that these operations are well-defined.

Let $\frac{a}{b} = \frac{a'}{b'}$ and $\frac{c}{d} = \frac{c'}{d'}$ then since $ab' = a'b$ and $cd' = c'd$ hold.

$$\begin{aligned}(ad+bc)b'd' &= adb'd' + bcb'd' \\ &= ab'dd' + bb'cd' \\ &= a'bdd' + bb'c'd \\ &= (a'd' + b'c')bd.\end{aligned}$$

This assert $\frac{ad+bc}{ba} = \frac{a'd'+b'c'}{b'a'}$ i.e. $\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'}$.

And since R is a commutative ring, obviously the multiplication is well-defined.

Clearly, these operations are commutative and Q is an Abelian group under addition; $+$ is additive, the additive identity is $\frac{0}{d}$ for all $d \in D$, and the additive inverse of $\frac{a}{d}$ is $\frac{-a}{d}$. And $\times$ is associative and distribute. Fluther Q has an identity $\frac{d}{d}$ for all $d \in D$.

Therefore Q is a commutative ring with identity.

KOKUYO LOOSE-LEAF 2-836ST 6 mm ruled x36 lines

Next we verify that R is embedding into Q. Define the map ι by

$$\iota : R \to Q \;;\; r \longmapsto \frac{rd}{d} \quad \text{where } d \in D.$$

we assert the function ι is well-defined.

And now,

$$\iota(r+s) = \frac{(r+s)d}{d} = \frac{rd+sd}{d} = \left(\frac{rd}{d}\right) + \left(\frac{sd}{d}\right) = \iota(r) + \iota(s),$$

$$\iota(r \cdot s) = \frac{rsd}{d} = \frac{rd}{d} \times \frac{sd}{d} = \iota(r) \cdot \iota(d).$$

Thus, ι is a homomorphism, also if $\iota(r) = \iota(s)$ then since $d \in D$,

$$\iota(r-s) \sim \frac{0}{d} \iff \frac{(r-s)d}{d} = \frac{0}{d} \iff (r-s)d^2 = 0 \iff r = s.$$

Then, ι is injective, so ι is isomorphism.

And by the First isomorphism theorem,

$$\iota(R) \simeq R/\ker \iota = R/0 \simeq R \qquad (\because \iota \text{ is injective})$$

So by identifing each $r \in R$ with $\iota(r)$, we can cosider R as a subring of Q.

Next we show that every $d \in D$ is a unit in Q.

For $\forall d \in D$ since $D \subset R \simeq \iota(R)$. d has the form $\frac{de}{e}$ for $e \in D$.

$$\frac{de}{e} \times \frac{e}{de} = \frac{dee}{ede} = \frac{e}{e} = (\text{identity})$$

(1) Since each $d \in D$ has a multiplicative inverse.

$$\frac{r}{d} = \frac{ref}{def} = \frac{re}{e} \times \frac{f}{df} = \frac{re}{e} \times \left(\frac{df}{f}\right)^{-1} = \frac{re}{e} \times \frac{d^{-1}f}{f} = r \cdot d^{-1} \quad \text{for all } r \in R, d \in D.$$

In paticular, if $D = R \setminus \{0\}$, then every non-zero element $\frac{r}{d}$ in Q has a multiplicative

inverse $\frac{d}{r}$.

Suppose, $\frac{d}{d} = \frac{0}{e}$ holds, then $de = 0$ since d has no zero divisor, $e = 0$ a contradiction Hence $1 \neq 0$ on Q.

Hence Q form the field.

(2) Let S be any commutative ring with identity and let $\varphi : R \to S$ be any ring isomorphism such that $\varphi(d)$ is a unit in S for all $d \in D$.

Extend φ to Φ by defing $\Phi : Q \to S$; $rd^{-1} \mapsto \varphi(r)\varphi(d)^{-1}$.

Then, Φ is well-defined since if $rd^{-1} = se^{-1}$ then $re = sd$ so $\varphi(re) = \varphi(sd)$, $\varphi(r) \cdot \varphi(e) = \varphi(s) \cdot \varphi(d)$. So, $\Phi(rd^{-1}) = \Phi(se^{-1})$ holds.

We show that Φ is ring homomorphism.

$$\Phi(rd^{-1} + se^{-1}) = \Phi\left((re+sd)\cdot(de)^{-1}\right) = \varphi(re+sd)\cdot\varphi(de)^{-1}$$

$$= \left(\varphi(r)\cdot\varphi(e) + \varphi(s)\cdot\varphi(d)\right)\varphi(e)^{-1}\cdot\varphi(d)^{-1}$$

$$= \varphi(r)\varphi(d)^{-1} + \varphi(s)\varphi(e)^{-1}$$

$$= \Phi(rd^{-1}) + \Phi(se^{-1})$$

Similary, $\Phi(rd^{-1} \cdot se^{-1}) = \Phi(rd^{-1}) \cdot \Phi(se^{-1})$.

Also, Φ is injective thus, Φ is ring homomorphism.

Cor 16 Let R be an integral domain and let Q be the field of fractions of R. If a field F' contains a subring R' isomorphic to R then the subfield of F' generated by R' is isomorphic

to Q.

Proof) Let $\varphi : R \to R'$ be a ring isomorphism. Especially since $R' \subset F$, $\varphi : R \to F'$ is an injective homomorphism.

Extend φ to Φ by defining $\Phi : Q \to F$; $rd^{-1} \longmapsto \varphi(r) \cdot \varphi(d)^{-1}$.

As in previous theorem, Φ is a injective isomorphism, so by the First isomorphism theorem

$Q \approx \Phi(Q)$ ($\because \ker\Phi = \{0\}$)

Let $X := \bigcap_{\substack{F' : \text{subfield} \\ R' \subset F'}} F'$ we show that $\Phi(Q) = X$.

Since, $Q \supset R$, $\Phi(Q) \supset \Phi(R) = \varphi(R) = R'$, $\Phi(Q)$ is a subring of F including R', $X \subset \Phi(Q)$.

Conversely for $r_1 \cdot r_2^{-1} \in Q$ since $R' \subset X$,

$\Phi(r_1 \cdot r_2^{-1}) = \varphi(r_1) \cdot \varphi(r_2)^{-1} = \varphi(r_1 \cdot r_2^{-1}) \in R' \subset X$

Thus, $X = \Phi(Q) \approx Q$

Thm 17 Chinese Remainder Theorem.

Let $A_1, A_2, \cdots, A_k$ be ideals in R. The map

$R \longrightarrow R/A_1 \times R/A_2 \times \cdots \times R/A_k$ defined by $r \mapsto (r+A_1, r+A_2, \cdots, r+A_k)$

is a ring homomorphism with kernel $A_1 \cap A_2 \cap \cdots \cap A_k$. If for each $i, j \in \{1,2,\cdots,k\}$ with $i \neq j$ the ideals A_i and A_j are comaximal, then this map is surjective and

$$R/(A_1 \cdot A_2 \cdots A_k) = R/(A_1 \cap A_2 \cap \cdots \cap A_k) \approx R/A_1 \times R/A_2 \times \cdots \times R/A_k.$$

Proof)

We prove by induction of k. First verify the case for $k=2$.

The map, $\varphi : R \to R/A_1 + R/A_2 \; ; \; r \mapsto (r+A_1, r+A_2)$ is clearly ring homomorphism and $\ker \varphi = A_1 \cap A_2$.

Thus, we have only to show that if A_1 and A_2 are comaximal, then φ is surjective and $A_1 \cap A_2 = A_1 \cdot A_2$.

Since, A_1, A_2 are comaximal, $A_1 + A_2 = R$ and $1 \in R$, there exists $x \in A_1, y \in A_2$ such that $x+y = 1$. Since $x \in A_1$, $x = 1-y \in 1+A_2$ holds.

$$\varphi(x) = (x+A_1, x+A_2) = (0+A_1, 1+A_2)$$

Similarly, $\varphi(y) = (1+A_1, 0+A_2)$ holds.

Now, for $(r_1+A_1, r_2+A_2) \in R/A_1 \times R/A_2$.

$$\varphi(r_2 x + r_1 y) = \varphi(r_2)\varphi(x) + \varphi(r_1)\varphi(y)$$

$$= (r_2+A_1, r_2+A_2)\cdot(0+A_1, 1+A_2) + (r_1+A_1, r_1+A_2)\cdot(1+A_1, 0+A_2)$$

$$= (0 + A_1, r_2 + A_2) + (r_1 + A_1, 0 + A_2)$$

$$= (r_1 + A_1, r_2 + A_2)$$

thus, φ is surjective.

Finally, since $A_1 \cdot A_2 \subset A_1 \cap A_2$ obviously holds, we show the reverse inclusion, let x and y as above.

For $c \in A_1 \cap A_2$,

$$c = c \cdot 1 = c \cdot (x + y) = xc + xy \in A_1 \cdot A_2 .$$

Thus, $A_1 \cap A_2 = A_1 \cdot A_2$ holds, complete the proof for the $k = 2$.

Next, for the general case, it is enough to show A_1 and $A_2 \cdot A_3 \cdots A_k$ are comaximal, for we have the result from the case $k = 2$.

Since, A_1 and A_i are comaximal and $1 \in R$ for each $i \in \{2, \cdots, k\}$.

there exists $x_i \in A_1$ and $y_i \in A_i$ such that $x_i + y_i = 1$.

Since $(x_i + y_i) + A_i = x_i + A_i$,

$$1 + A_1 = (x_2 + y_2) \cdot (x_3 + y_3) \cdot \cdots \cdot (x_k + y_k) + A_1$$

$$= ((x_2 + y_2) + A_1) \cdot ((x_3 + y_3) + A_1) \cdot \cdots \cdot ((x_k + y_k) + A_1)$$

$$= (y_2 + A_1) \cdot (y_3 + A_1) \cdot \cdots \cdot (y_k + A_1)$$

$$= (y_2 \cdot y_3 \cdot \cdots \cdot y_k) + A_1 \in (A_2 \cdot A_3 \cdot \cdots \cdot A_k) / A_1$$

Thus, $1 \in A_2 \cdot A_3 \cdot \cdots \cdot A_k \subset A_1 + A_2 \cdot A_3 \cdots A_k$ and therefore $A_1 + A_2 \cdots A_k = R$.

Cor 18 Let n be a positive integer and let $p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}$ be its factorization into powers of distinct primes. Then

$$\mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/p_1^{d_1}\mathbb{Z}) \times (\mathbb{Z}/p_2^{d_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_k^{d_k}\mathbb{Z}),$$

as a ring so in particular we have the following isomorphism of multiplicative groups.

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{d_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{d_2}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k^{d_k}\mathbb{Z})^\times$$

Proof)

Since $p_1^{d_1}, p_2^{d_2}, \cdots, p_k^{d_k}$ are pairwise relatively prime, by Chinese Remainder Theorem

$$p_1^{d_1}\mathbb{Z} \cap p_2^{d_2}\mathbb{Z} \cap \cdots \cap p_k^{d_k}\mathbb{Z} = (p_1^{d_1} \cdot p_2^{d_2} \cdots p_k^{d_k})\mathbb{Z} = n\mathbb{Z}$$

moreover, $\mathbb{Z}/n\mathbb{Z} \approx (\mathbb{Z}/p_1^{d_1}\mathbb{Z}) \times (\mathbb{Z}/p_2^{d_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_k^{d_k}\mathbb{Z})$.

To show that $(\mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/p_1^{d_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{d_2}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k^{d_k}\mathbb{Z})^\times$

If we verify $(R \times S)^\times = R^\times \times S^\times$, it is obviously there exists isomorphism from $(R \times S)^\times$ to $R^\times \times S^\times$. Hence $\left((\mathbb{Z}/p_1^{d_1}\mathbb{Z}) \times \cdots (\mathbb{Z}/p_k^{d_k}\mathbb{Z})\right)^\times \approx (\mathbb{Z}/p_1^{d_1}\mathbb{Z})^\times \times \cdots \times (\quad)^\times$.

and since $(\mathbb{Z}/n\mathbb{Z})^\times \approx \left((\mathbb{Z}/p_1^{d_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_k^{d_k}\mathbb{Z})\right)^\times$ holds for multiplicative group the statement holds.

Thus, we verify $(R \times S)^\times = R^\times \times S^\times$ for any rings.

$\forall (x, y) \in R^\times \times S^\times \; \exists (a, b) \in R \times S$ such that

$$(x, y) \cdot (a, b) = (a, b) \cdot (x, y) = 1$$

thus, $xa = ax = 1$ and $yb = by = 1$

Thus, x and y are unit of R and S.

Prop 1 Every ideal in a Euclidean Domain is pricipal. More precisely, if I is any nonzero ideal in the Euclidian Domain R then $I = (d)$, where d is any nonzero element of I of minimal norm.

Proof.) If $I = 0$, the assertion is obvious. Thus assume $I \neq 0$.

Let d be any nonzero element of I of minimal norm.

We prove that $(d) = I$. Since $(d) \subset I$ is obvious, we show that the reverse inclusion.

Let $a \in I$ since R is an Euclidian norm. $\exists q, r \in R$ $a = qd + r$ with $d \neq 0$ and $r = 0$ or $N(r) < N(d)$.

Now, $r = a - qd \in I$ so by minimality of $N(d)$, $N(r) \not< N(d)$ thus we must have $r = 0$. Thus, $a = qd \in (d)$.

Prop 2. If a and b are nonzero element in the commutative ring R such that the ideal generated by a and b is a pricipal ideal (d), then d is a greatest common divisor of a and b.

Proof)
Since $(d) = (a, b)$ holds, $(a) \subset (d)$ and $(b) \subset (d)$ hold.

Thus, for some x and y, $a = dx$ and $b = dy$ i.e. $d \mid a$ and $d \mid b$ hold.

Let $d' \in R$ with $d' \mid a$ and $d' \mid b$ then clearly $(a) \subset (d')$ and $(b) \subset (d')$ moreover $(a, b) \subset (d')$. Hence, $d' \mid d$ holds.

Therefore, d' is a greatest common divisor of a and b.

Prop 3. Let R be an integral domain. If two elements d and d' of R generated the same pricipal ideal, i.e. $(d) = (d')$, then $d' = u \cdot d$ for some unit u in R. In paticular, if d and d' are both greatest common divisors of a and b, then $d' = ud$ for some unit u.

Proof) If either $d = 0$ or $d' = 0$ then the result is obvious. So assume $d \neq 0$ and $d' \neq 0$.

Since, $d \in (d')$ $\exists x \in R$, $d = d'x$. Also since $d' \in (d)$, $d' = dy$ for some y. Thus, $d = dyx$ i.e. $d(1 - yx) = 0$.

Since R has no zero divisor and $d \neq 0$, we must have $yx = 1$ thus, x and y are units, so the first assertion follows.

Thm 4 Let R be a Euclidian Domain and let a and b be nonzero element of R. Let $d = r_n$ be the last nonzero ramainder in the Euclidian Algorithm for a and b. Then

(1) d is a greatest common divisor of a and b. Then

(2) the pricipal ideal (d) is the ideal generated by a and b. In paticular, d can be written as an R-linear combination of a and b, i.e. there are elements x and y in R such that $d = ax + by$.

Proof.)

If (2) holds, by prop 2 we have d is the greatest common divisor of a and b.

Thus, for (1) and (2) it is enough to show that $(d) = (a, b)$.

First we prove that $r_k \mid r_{k-1}$ and $r_n \mid r_k$ for $k = n, n-1, \cdots, 1$ by induction.

By the $(n+1)$st equation in the Euclidian Algorithm, $r_n \mid r_{n-1}$ and clearly $r_n \mid r_n$.

Thus, it is true for $k = n$.

Next, we assume $r_n \mid r_k$ and $r_n \mid r_{k+1}$. By the $(k+1)$st equation,

$r_{k-1} = q_k \cdot r_k + r_{k+1}$. By assumption, there exists α and β such that $r_k = r_n \alpha$, $r_{k+1} = r_n \beta$

Thus, $r_{k-1} = q_k \cdot r_n \cdot \alpha + r_n \cdot \beta = (q_k \alpha + \beta) r_n$ so, $r_n \mid r_{k-1}$.

Hence, $r_n \mid r_{k+1}$ and $r_n \mid r_k$ for all k.

Now by the 1st equation, $r_0 \mid b$ and moreover $r_0 \mid a$ thus, $r_n \mid b$ and $r_n \mid a$.

This assert $(a, b) \subset (d)$.

To prove that $r_n \in (a, b)$. First show that $r_{k-1}, r_k \in (a, b)$ for $k = 1, 2, \cdots n$, by induction. By the 0th equation $r_0 = a - q_0 b \in (a, b)$, and by the 1st equation $r_1 = b - q_1 r_0 \in (a, b)$. Thus this is true for $k = 1$.

Next we assume $r_{k-1}, r_k \in (a, b)$. Then by the $(k+1)$st equation

$r_{k+1} = r_{k-1} - q_{k+1} \cdot r_k \in (r_{k-1}, r_k) \subset (a, b)$ Therefore, $r_{k+1} \in (a, b)$ holds.

and therefore, $(r_n) \subset (a, b)$, $(r_n) = (a, b)$ holds.

Prop 5 Let R be an integral domain that is not a field. If R is a Euclidean Domain then there are universal side divisors in R.

Proof.) Let R be a Euclidean Domain with respect to some norm N and let $u \in R \setminus \widetilde{R}$ of minimal norm.

For $x \in R$ since R is Euclidean domain there exists $q, r \in R$ such that $x = qu + r$, $u \neq 0$ and $r = 0$ or $N(r) < N(u)$ hold.

If $r = 0$ then $r \in \widetilde{R}$.

If $N(r) < N(u)$ by minimality of $N(u)$. $r \notin R \setminus \widetilde{R}$ thus, $r \in \widetilde{R}$.

Hence, $x - r = q \cdot u$ i.e. $u \mid x - r$ for $\forall x \in R \; \exists r \in \widetilde{R}$

Prop 6 Let R be a Pricipal ideal Domain and let a and b be non-zero elements of R. Let d be a generater for the pricipal ideal generated by a and b. Then

(1) d is a greatest common divisor of a and b

(2) d can be written as an R-linear combination of a and b, i.e., there are elements x and y in R with $d = ax + by$.

(1) By prop 2 obviously assert.

(2) By $(d) = (a, b)$ iff $d \in (a, b)$, obviously holds.

(3) By prop 3 manifestly holds.

Prop 7. Every nonzero prime ideal in a Principal Ideal Domain is a maximal ideal.

Proof.) Let R be a Principal Ideal Domain and let (p) be a non-zero prime ideal in R.

Let $I = (m)$ be any ideal of R such that $(m) \supset (p)$.

We show that (p) is a maximal ideal i.e. $I = (p)$ or $I = R$.

Since, $p \in (m)$ $\exists r \in R$ $p = rm$ and moreover since (p) is a prime ideal, either $r \in (p)$ or $m \in (p)$ must hold.

If $(m) \subset (p)$ then $I = (p)$.

If $r \in (p)$ then there exists $s \in R$ such that $r = ps$.

Since $p = rm = psm$ and p is non-zero divisor, $sm = 1$

Thus, m is a unit so by prop 7.9 $(m) = I = R$.

Cor 8. If R is any commutative ring such that the polynomial ring $R[x]$ is a Principal Ideal Domain (or a Euclidean Domain), then R is necessarily a field.

Proof). (x) is the non-zero prime ideal in $R[x]$ then by prop 7. (x) is the maximal ideal moreover by Thm 7.12 $R[x]/(x)$ form the field.

Now, it is enough to verify $R[x]/(x) \simeq R$.

Let φ be the function from $R[x]$ to R which assign the $p(x)$ the $p(0)$. Then clearly φ is isomorphism. and $\ker \varphi = (x)$ then by first isomorphism theorem $R[x]/(x) \simeq R$.

Therefore, R form the field.

Prop 9. The integral domain R is a P.I.D iff R has a Dedekind-Hasse norm. (The $\Rightarrow$ will be proved in the cor 16.)

Proof) ($\Leftarrow$) Suppose R has a Dedekind-Hasse norm N. Let I be any non-zero ideal of R and let b be a non-zero element of I such that $N(b)$ is minimal in I. Then clearly $(b) \subset I$ so we show inverse inclusion.

Let $\forall a \in I$. If $a = 0$ then $(a) \subset (b)$ so assume $a \neq 0$.

Since N is Dedekind-Hasse norm, $a \in (b)$ or $\exists x \in (a, b)$. $x \neq 0$ and $0 < N(x) < N(b)$.

By minimality of $N(b)$, if letter holds contradicts to $x \notin I$ but $x \in (a,b)$ then $a \in (b)$.

Therefore, $I = (b)$.

Prop 10 In an integral domain a prime element is always irreducible.

Proof) Let p be a prime element with $ab = p$. Then $ab \in (p)$ thus, $(a) = (p)$ or $(b) = (p)$, for some r, $a = pr$ holds. Therefore $p = ab = prb$. thus, $rb = 1$, b is a unit.

Thus, p is irreducible.

Prop 11. In a Principal Ideal Domain a non-zero element is a prime iff it is irreducible.

Proof) Previous theorem assert prime element is irreducible. We show conversely, suppose p is irreducible. Let M be an ideal containg (p) with $M = (m)$. Then for some r, $p = rm$. Since p is irreducible, r or m is an unit that is, $(p) = (m)$ or $(p) = R$. This assert (p) is a maximal ideal. Then by Cor 7.14 (p) is a prime ideal. p is prime.

Prop 12. In a Unique Factorization Domain a nonzero element is a prime iff it is irreducible.

Proof) By thm 10, every non-zero prime element is irreducible. We show conversely, suppose p is irreducible of U.F.D. R. We assert for $a, b \in R$ $ab \in (p)$ implies $a \in (p)$ or $b \in (p)$.

Suppose $ab \in (p)$ for $a, b \in R$ then $ab = rp$ for some r.

Since $a, b \in R$, $a = p_1 \cdots p_n$, $b = q_1 \cdots q_m$ with every p_i and q_j is irreducible.

Since $ab = rp$ and p is irreducible, p is associate to some p_i or q_j i.e. $p = u p_i$ for unit u w.l.g. Then $a \in (p_1) = (p)$ holds.

Therefore, p is a prime element.

Prop 1 Let R be an integral domain. Then

(1) degree $f(x)g(x)$ = degree $f(x)$ + degree $g(x)$ if $f(x), g(x)$ are nonzero,

(2) the units of $R[x]$ are just the units of R,

(3) $R[x]$ is an integral domain.

Prop 2. Let I be an ideal of the ring R and let $(I) = I[x]$ denote the ideal of $R[x]$ generated by I. Then $R[x]/(I) \approx (R/I)[x]$.

In poticular, if is a prime ideal of R then (I) is a prime ideal of $R[x]$.

Proof) Let $\varphi : R[x] \longrightarrow (R/I)[x]$; $\sum_{0\le i\le n} a_i x_i \longmapsto \sum_{0\le i\le n} (a_i+I) x_i$. Then clearly φ is surjective. We assert φ is ring homomorphism.

$$\varphi\left(\sum_{0\le i\le n} a_i x_i + \sum_{0\le i\le m} b_i x_i\right) = \varphi\left(\sum_{0\le i\le m} (a_i+b_i) x_i\right)$$

$$= \sum_{0\le i\le m} (a_i+b_i)+I \; x_i$$

$$= \sum_{0\le i\le n} (a_i+I)x_i + \sum_{0\le i\le m} (b_i+I) x_i$$

$$= \varphi\left(\sum_{0\le i\le n} a_i \cdot x_i\right) + \varphi\left(\sum_{0\le i\le m} b_i \cdot x_i\right)$$

$$\varphi\left(\sum_{0\le i\le n} a_i \cdot x_i \cdot \sum_{0\le i\le m} b_i x_i\right) = \varphi\left(\sum_{0\le k\le n+m} \left(\sum_{0\le i\le k} a_i \cdot b_{k-i}\right) x_k\right)$$

$$= \sum_{0\le k\le n+m} \left(\sum_{0\le i\le k} a_i \cdot b_{k-i}\right)+I \cdot x_k$$

$$= \sum_{0\le k\le n+m} \sum_{0\le i\le k} (a_i \cdot b_{k-i}+I) \cdot x_k$$

$$= \sum_{0\le k\le n+m} \sum_{0\le i\le k} (a_i+I)(b_{k-i}+I)\; x_k$$

$$= \sum_{0\le i\le n} (a_i+I) x_i \cdot \sum_{0\le i\le m} (b_i+I) \cdot x_i$$

KOKUYO LOOSE-LEAF A-836BT 6 mm ruled 26 lines

$$= \varphi\Big(\sum_{0\le i\le n} a_i x_i\Big)\cdot \varphi\Big(\sum_{0\le i\le m} b_i x_i\Big).$$

Thus, φ is ring homomorphism. And clearly $\ker\varphi = (1)$.

Suppose that I is a prime ideal, by prop 7.13 R/I is an integral domain, so is $R/I[x]$. And by previous fact, $R[x]/(1)$ is also an integral domain. Thus, (1) is an integral domain.

Thm3. Let F be a field. The polynomial ring $F[x]$ is a Euclidean domain. Specifically, if $a(x)$ and $b(x)$ are two polynomials in $F[x]$ with $b(x)$ nonzero, then there are unique $q(x)$ and $r(x)$ in $F[x]$ such that $a(x) = q(x)b(x) + r(x)$ with $r(x) = 0$ or degree $r(x)$ < degree $b(x)$.

Proof). If $a(x) = 0$, take $q(x) = r(x) = 0$. Thus, assume $a(x) \neq 0$.

Let $n := \deg a(x)$ and $m := \deg b(x)$.

If $n < m$, take $q(x) = 0$ and $r(x) = a(x)$. Then we have the result.

If $n \ge m$, we prove by induction on n. Write, $a(x) = a_n x^n + \cdots + a_0$, and $b(x) = b_m x^m + \cdots + b_0$. Note that $a_n b_m \neq 0$.

When, $n = 0$, $a(x) = a_0$ and by $m \le n$, $b(x) = b_0 \neq 0$. Take $q(x) = \frac{a_0}{b_0}$ $(:= a_0 b_0^{-1})$ and $r(x) = 0$, then $a(x) = q(x)b(x) + r(x)$ holds.

If $n > 0$. Let $a'(x) := a(x) - \frac{a_n}{b_m} x^{n-m} b(x)$. Then $\deg a'(x) < \deg a(x) = n$, by induction $\exists q'(x), r(x)$ $a'(x) = q'(x)b(x) + r(x)$ with $r(x) = 0$ or $\deg r(x) < \deg b(x)$.

Now, we define $q(x) = q'(x) + \frac{a_n}{b_m} x^{n-m}$ then, $a(x) = q(x)b(x) + r(x)$ where $r(x) = 0$ or $\deg r(x) < \deg b(x)$.

Next, we pove the uniqueness. Suppose, $a(x) = q_1(x)b(x) + r_1(x) = q_2(x)b(x) + r_2(x)$ with $r_1(x) = 0$ or $\deg r_1(x) < \deg b(x)$, and $r_2(x) = 0$ or $r_2(x) < \deg b(x)$.

If $r_1(x) \neq 0$ and $r_2(x) \neq 0$, we obtain $\deg\big((q_1(x) - q_2(x))\, b(x)\big) = \deg(r_2(x) - r_1(x)) < 0$. Hence, if $q_1(x) - q_2(x)$ is nonzero, $\deg(q_1(x) - q_2(x)) + \deg(b(x)) = \deg\big((q_1(x) - q_2(x))\, b(x)\big) < 0$, a contradiction. Thus, $q_1(x) = q_2(x)$ moreover, $r_1(x) = r_2(x)$. The other cases mimik the proof of this case.

Cor 4 If F is a field, then $F[x]$ is a P.I.D. and a U.F.D.

Proof) By previous theorem $F[x]$ is a Euclidean domain thus, $F[x]$ is a P.I.D and a U.F.D..

Prop 5 Gauss's Lemma.

Let R be a U.F.D. with field of factorization F and let $p(x) \in R[x]$. If $p(x)$ is reducible in $F[x]$ then $p(x)$ is reducible in $R[x]$. More precisely, if $p(x) = A(x)\,B(x)$ for some nonconstant polynomials $A(x), B(x) \in F[x]$, then there are nonzero elements $r, s \in F$ such that $rA(x) = a(x)$ and $sB(x) = b(x)$ both lie in $R[x]$ and $p(x) = a(x)b(x)$ is a factorization in $R[x]$.

Proof) Suppose $p(x) = A(x) \cdot B(x)$ where $A(x)$ and $B(x)$ are nonunit, we have the form $p(x) = \Big(\sum_{0 \le i \le n} \frac{a_i}{c_i} x_i\Big)\Big(\sum_{0 \le i \le m} \frac{b_i}{c'_i} x_i\Big)$ thus for $d := c_0 \cdot c_1 \cdot \cdots \cdot c_n \cdot c'_0 \cdot c'_1 \cdot \cdots \cdot c'_m \in R \setminus \{0\}$, $d\,p(x) = a'(x)\cdot b'(x)$ $\cdots$ (*) for some $a'(x), b'(x) \in R[x]$ and note that $a'(x) \in F\cdot A(x)$.

If $d \in R^\times$, for some d', $p(x) = d'\,a'(x)\,b'(x)$ thus $p(x)$ is reducible.

KOKUYO LOOSE-LEAF A-836BT 6 mm ruled x36 lines

If $a \notin R^\times$, since R is U.F.D., $a = p_1 \cdots p_n$, where each p_i is irreducible in R.

By prop 8.12 each (p_i) is a prime ideal, then by prop 2, $(p_i)[x]$ is a prime ideal, hence by prop 7.13, $R[x]/(p_i)[x]$ is an integral domain.

Now by (*), $0 + (p_i)[x] = (a'(x)\ b'(x)) + (p_i)[x] = (a'(x) + (p_i)[x])(b'(x) + (p_i)[x])$.

So we assume, $a'(x) \in (p_i)[x]$ w.l.o.g.. Since $a'(x) = \sum_{0 \le j \le n} a_j(x) \cdot p_i \cdot x^j$ and $p_i \in F$, $p_i^{-1} \in F$, $p_i^{-1} \cdot a'(x) \in R[x]$ for every i.

Therefore for (*) we multiplying $p_1, p_2, \cdots, p_n$ from left, we have $p(x) = a(x)\ b'(x)$, where $a(x) = p_n^{-1} \cdots p_i^{-1} a'(x) \in R \subseteq F$ and $b'(x) \in R \subseteq F$. Then, $a(x) \in F \cdot A(x)$ and $b(x) \in F \cdot B(x)$ and $a(x)$ and $b(x)$ are noncunit.

Cor 6 Let R be a U.F.D., let F be its field of fractions and let $p(x) \in R[x]$. Suppose the greatest common divisor of the coefficients of $p(x)$ is 1. Then $p(x)$ is irreducible in $R[x]$ iff it is irreducible in $F[x]$. In paticular, if $p(x)$ is a manic polynomial that is irreducible in $R[x]$, then $p(x)$ is irreducible in $F[x]$.

Proof) By Gauss's lemma ($\Rightarrow$) is manifestly. We piove the conversly by contraposition.

By assumption, $\exists a(x), b(x) \in R[x] \setminus R^\times$ with $p(x) = a(x) \cdot b(x)$. Since the g.c.d. of coefficient of $p(x)$ is 1, the g.c.d. of coeffient of $a(x)$ and $b(x)$ are 1. This assent if $a(x) \in R$, $a(x) = 1$.

Thus, $a(x), b(x) \in R[x] \setminus R$ moreover, $a(x), b(x) \in F[x] \setminus F^\times$ this shows, $p(x)$ is reducible in $F[x]$.

Thm 7. R is a U.F.D. iff $R[x]$ is a U.F.D..

Proof).

($\Rightarrow$) Let $F := (R\setminus\{0\})^{-1}\cdot R$ be a quotient field and let $p(x) \in R[x] \setminus (\{1\}\cup R^\times)$.

Since, the g.c.d., d, of all coefficients of $p(x)$ is not 1 then we have $p(x) = d\cdot p'(x)$ and the g.c.d. of $p'(x)$ is 1 and since $d\in R$, d has the unique factorization. Thus, we assume that the g.c.d. of $p(x)$ is 1.

Since, $F[x]$ is a U.F.D., $p(x)$ has the unique factorization $f_1(x)f_2(x)\cdots f_n(x)$ in $F(x)$. By Gauss's lemma, $\exists g_1,\cdots g_n \in F\setminus\{0\}$, $g_i f_i(x) \in R[x]$ for each i and, $p(x) = g_1 f_1(x)\cdots g_n f_n(x)$. Since the g.c.d. of all coefficient of $p(x)$ is 1, by Cor 6, $g_i f_i[x]$ is irreducible in $R[x]$. Hence we obtain a factorization.

Next, we show the uniqueness. Suppose that $p(x)$ has factorizations $g_1(x)\cdots g_n(x)$ and $g'_1(x)\cdots g_{n'}(x)$ in $R[x]$. Then since the g.c.d. of all coefficient of $p(x)$ is 1, by Cor 6, $g_i(x)$, $g_i'(x)$ are irreducible in $F[x]$. Since, $F[x]$ is U.F.D., $n=m$ and $g_i(x) = u_i\cdot g_i'(x)$ for every i and $u_i = \frac{a_i}{b_i}$, $a_i, b_i \in R\setminus\{0\}$. Since $a_i = u_i\cdot b_i$, by prop 8.3, $\exists \sigma_i \in R^\times$, $a_i = \sigma_i\cdot b_i$ thus, u_i is an unit in R. This assert a factorization of $p(x)$ is unique, $R[x]$ is a U.F.D..

($\Leftarrow$) Let $r\in R\setminus(\{0\}\cup R^\times)$. Since $R[x]$ is U.F.D., r has the unique factorization $f_1(x)\cdots f_n(x)$. By $0 = \deg(r) = \deg(f(x)) + \cdots + \deg(f_n(x))$, $\deg(f_i(x)) = 0$, $f_i(x)\in R\setminus(\{0\}\cup R^\times)$ for every i. Thus, $f_i(x)$ is irreducible.

KOKUYO COSE-LEAF A-836DT 6 mm ruled × 36 lines

Cor 8. If R is a U.F.D., then a polynomial ring in an arbitrary number of variables with coefficients in R is also a U.F.D..

Proof). For a polynomial with finitely variables, $R[x_1, \cdots, x_n]$ becomes a U.F.D., by induction, using thm 7.

Prop 9. Let F be a field and let $p(x) \in F[x]$. Then $p(x)$ has a factor of degree one iff $p(x)$ has a root in F, i.e. there is an $\alpha \in F$ with $p(\alpha) = 0$.

Proof). By assumption, $p(x)$ has the form $(a_1 x + a_0) q(x)$ where $q(x) \in F[x]$, $a_1 \in F \setminus \{0\}$ and $a_1 \in F$. Since F is a field, $p(x) = a_1 \cdot q(x) \cdot \left(x + \frac{a_0}{a_1}\right)$ thus, $p\left(-\frac{a_0}{a_1}\right) = 0$.

Conversely, suppose $\exists \alpha \in F$, $p(\alpha) = 0$. Since $x - \alpha \in F[x]$ and $F[x]$ is a Euclidean domain, $\exists q(x), r \in F[x]$, $p(x) = q(x)(x-\alpha) + r$. Thus, since $p(\alpha) = 0$, $r = 0$, Hence, $p(x) = q(x) \cdot (x - \alpha)$.

Thm 10. A polynomial of degree two or three over a field F is reducible iff it has a root in F.

Proof)

(i) degree 2.

($\Rightarrow$) Let $p(x) = a_2 x^2 + a_1 x + a_0$ with $a_2 \in F \setminus \{0\}$, $a_2, a_1 \in F$. Since p is reducible, $\exists f_1(x), f_2(x) \in F[x] \setminus F$ $p(x) = f_1(x) \cdot f_2(x)$. Then by $2 = \deg(p(x)) = \deg(f_1(x)) + \deg(f_2(x))$, $\deg(f_1(x)) = 1$ then by previous proposition $p(x)$ has root in F.

($\Leftarrow$) Similar to the reverse in previous proposition.

(ii) degree 3. Mimic the case of the proof of degree 2.

Prop11. Let $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ be a polynomial of degree n with integer coefficients. If $\frac{r}{s} \in \mathbb{Q}$ is in lowest terms (i.e. r and s relatively prime integers) and $\frac{r}{s}$ is a root of $p(x)$, then r divides the constant term and s divides the leading coefficient of $p(x)$: $r \mid a_0$ and $s \mid a_n$. In paticular, if $p(x)$ is a monic polynomial with integer coeffients and $p(d) \neq 0$ for all integers d dividing the constant term of $p(x)$, then $p(x)$ has no roots in $\mathbb{Q}$.

Proof).

(First assertion)

Since, $0 = p\left(\frac{r}{s}\right) = a_n \left(\frac{r}{s}\right)^n + \cdots + a_1 \left(\frac{r}{s}\right) + a_0$, multiplying s^n then we have, $0 = a_n r^n + \cdots + a_1 \cdot r \cdot s^{n-1} + a_0 \cdot s^n$ moreover, $a_n \cdot r^n = s \cdot -(a_{n-1} \cdot r^{n-1} + \cdots + a_1 \cdot s^{n-1})$.

This assert, $(a_n r^n) \subset (s)$ and since $(r) \cap (s) = 1$ we have $(a_n) \subset (s)$.

Similarly, since we have $a_0 s^n = r \cdot -(a_n r^{n-1} + \cdots + a_1 s^{n-1})$, we have $(a_0) \subset (r)$.

(Second assertion)

Suppose not, $p(x)$ has roots $q = \frac{r_1}{r_2}$ in $\mathbb{Q}$ with $r_1 \in \mathbb{Z}$, $r_2 \in (\mathbb{Z} \setminus (\{0\} \cup \mathbb{Z}^\times)) \cup \{1\}$ and $p(q) = 0$. Then by first assertion we obtain, $(a_0) \subset (r_1)$ and $(1) \subset (r_2)$, so $r_2 = 1$, and by assumption, $p(r_1) \neq 0$. However, $p(r_1) = p\left(\frac{r_1}{r_2}\right) = p(q) = 0$, a contradiction.

Prop 12. Let I be a proper ideal in the integral domain R and let $p(x)$ be a nonconstant monic polynomial in $R[x]$. If the image of $p(x)$ in $(R/I)[x]$ cannot be factored in $(R/I)[x]$ into two polynomials of smaller degree, then $p(x)$ is irreducible in $R[x]$.

Proof) Suppose that $p(x)$ is irreducible in $R[x]$, i.e., $\exists\, a(x), b(x) \in R[x] \setminus R^\times$ with $p(x) = a(x) \cdot b(x)$. Now, we pick $a(x)$ and $b(x)$ as monic and non-constant.

KOKUYO LOOSE-LEAF

Let a_n and b_m be the leading term of $a(x)$ and $b(x)$, respectively.

(i) monic.

Since $a_n \cdot a_m = 1$, $p(x) = a(x) \cdot b(x) = a_n \left(x^n + \frac{a_{n-1}}{a_n} x^{n-1} + \cdots \right) \cdot b_m \left(x^m + \frac{b_{m-1}}{b_m} x^{m-1} + \cdots \right)$.

$= \left(x^n + \frac{a_{n-1}}{a_n} x^{n-1} + \cdots \right) \left(x^m + \frac{a_{m-1}}{a_m} x^{m-1} + \cdots \right)$.

(ii) non-constant

Since $a_n \cdot a_m = 1$, $a_n, a_m \in R^\times$. If $a(x) \in R$ then, $a(x) \in R \setminus R^\times$ and $a(x) = a_n$, a contradiction.

Thus, we can pick $a(x)$ and $b(x)$ as monic and non-constant.

Since, φ is a ring homomorphism, $\varphi(p(x)) = \varphi(a(x)) \cdot \varphi(b(x))$, moreover, $\deg(\varphi(p(x))) = \deg(\varphi(a(x))) + \deg(\varphi(b(x)))$ this assert $\varphi(p(x))$ has a factorization of two polynomials of smaller degree.

Prop13. Eisenstein's Criterion

Let P be a prime ideal of the integral domain R and let $f(x) = x^n + a_{n-1} x^n + \cdots + a_0$ be a polynomial in $R[x]$ (here $n \geq 1$). Suppose $a_{n-1}, \cdots, a_0$ are all elements of P and suppose a_0 is not an element of P^2. Then $f(x)$ is irreducible.

Proof) If not, $f(x)$ has a form $a(x) \cdot b(x)$ where $a(x), b(x) \in R[x] \setminus R^\times$. As we have seen in previous proposition let $a(x) = \sum_{0 \leq i \leq k} \alpha_i \cdot x^i$ and $b(x) = \sum_{0 \leq j \leq \ell} \beta_j x^j$ with $k, \ell \geq 1$ and $\alpha_k = \beta_\ell = 1$.

Consider a map $\varphi : R[x] \to (R/P)[x]$; $\sum b_i \cdot x_i \mapsto \sum \varphi(b_i) \cdot x_i$. Since φ is homomorphic and every coefficient of $f(x)$ but the leading turm is in P, $x^n = \left(\sum_{0 \leq i \leq k} (\alpha_i + P) \cdot x^i \right) \left(\sum_{0 \leq j \leq \ell} (\beta_j + P) \cdot x^j \right)$.

moreover, we have $0+P=(\alpha_0+P)(\beta_0+P)=\alpha_0\beta_0+P$ thus, $\alpha_0\beta_0\in P$ and since P is prime $\alpha_0\in P$ or $\beta_0\in P$. Assume that $\alpha_0\in P$ w.l.o.g.

Since $n\geq 2$, $0+P=(\alpha_0+P)(\beta_1+P)+(\alpha_1+P)(\beta_0+P)=(0+P)+(\alpha_1\beta_0+P)$ thus we have $\alpha_1\beta_0\in P$, this assent $\alpha_1\in P$ or $\beta_0\in P$. However, if $\beta_0\in P$, $a_0=\alpha_0\beta_0\in P^2$, a contradiction. Thus, $\alpha_1\in P$, through inductive steps, we have $\alpha_i\in P$ for $i=1,\cdots,k-1$.

Now, the coefficient of x^k in $f(x)$ is $\left(\sum_{0\leq i\leq k-1}(\alpha_i\beta_{k-i})+P\right)+(\beta_0+P)$ thus, $\beta_0\in P$, a contradiction.

Cor 14. Let p be a prime in $\mathbb{Z}$ and let $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_0\in\mathbb{Z}[x]$, $n\geq 1$. Suppose p divides a_i for all $i\in\{0,1,\cdots,n-1\}$ but that p^2 does not divide a_0. Then $f(x)$ is irreducible in both $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$.

Proof) By previous lemma, $f(x)$ is irreducible in $\mathbb{Z}[x]$ and by Cor 6 the same is true in $\mathbb{Q}[x]$.

Prop15 The maximal ideals in $F[x]$ are the ideals $(f(x))$ generated by irreducible polynomials $f(x)$. In particular, $F[x]/(f(x))$ is a field iff $f(x)$ is irreducible.

Proof) Since $F[x]$ is a Euclidean domain, every maximal ideal is prime and every irreducible is prime, the first assertion holds. The second assertion follows by $F[x]/(f(x))$ is a field iff $(f(x))$ is maximal.

Prop16. Let $g(x)$ be nonconstant element of $F[x]$ and let $g(x) = f_1(x)^{n_1} \cdot f_2(x)^{n_2} \cdots f_k(x)^{n_k}$ be its factorization into irreducibles, where the $f_i(x)$ are distinct. Then we have the following isomorphism of rings:

$$F[x]/(g(x)) \cong F[x]/(f_1(x)^{n_1}) \times \cdots \times F[x]/(f_k(x)^{n_k}).$$

Proof) Since R is P.I.D., for $i \neq j$, we have g.c.d. $(f_i(x)^{n_i}, f_j(x)^{n_j}) = 1$, we obtain $(f_i(x)^{n_i}) + (f_j(x)^{n_j}) = (f_i(x)^{n_i}, f_j(x)^{n_j}) = (\text{g.c.d.}(f_i(x)^{n_i}, f_j(x)^{n_j})) = R$ thus, $(f_i(x)^{n_i})$ are comaximal. Therefore, by Chinese Remainder theorem we have the given isomorphism.

Prop17. If the polynomial $f(x)$ has roots $\alpha_1, \cdots, \alpha_k$ in F (not necessarily distinct), then $f(x)$ has $(x-\alpha_1)\cdots(x-\alpha_k)$ as a factor. In particular, a polynomial of degree n in one variable over a field F has at most n roots in F, even counted with multiplicity.

Proof) Both of the assertions derived from prop 9.

Prop18. A finite subgroup of the multiplicative group of a field is cyclic. In particular, if F is a finite field, then the multiplicative group $F^\times$ of nonzero elements of F is a cyclic group.

Proof) Let F be a field and let $G \subseteq F^\times$ be a finite group. By Fundamental theory of finitely generated Abelian group, $G \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$ with $n_k | \cdots | n_1$.

Now, by Lagrange's theorem, if d divide order of group H, H contains more than or equals to d elements of order dividing d. Since, $n_k \mid |\mathbb{Z}/n_i\mathbb{Z}|$ for all i, each $\mathbb{Z}/n_i\mathbb{Z}$ contains n_k elements of order dividing n_k.

If $k > 1$, for polynomial $x^{n_k} - 1 \in F[x]$ has more than n_k^k roots however by prop17 roots of $x^{n_k} - 1$ is less than equals to n_k. Thus $k = 1$, G is cyclic.

Cor19. Let p be a prime. The multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ of nonzero residue classes mod p is cyclic.

Proof). Since $\mathbb{Z}/p\mathbb{Z}$ is a finite field, this follows from previous proposition.

Cor20 Let $n \geq 2$ be an integer with factorization $n = p_1^{d_1} \cdot p_2^{d_2} \cdots p_r^{d_r}$ in $\mathbb{Z}$, where $p_1, \cdots, p_r$ are distinct primes. We have the following isomorphism of multiplicative groups:

(1) $(\mathbb{Z}/n\mathbb{Z})^\times \simeq (\mathbb{Z}/p_1^{d_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_r^{d_r}\mathbb{Z})^\times$.

(2) $(\mathbb{Z}/2^d\mathbb{Z})^\times$ is the direct product of a cyclic group of order 2 and a cyclic group of order 2^{d-2}, for all $d \geq 2$.

(3) $(\mathbb{Z}/p^d\mathbb{Z})^\times$ is a cyclic group of order $p^{d-1}(p-1)$, for all odd primes p.

Proof)

(1) Prove in Prop 7.18.

(2) Clearly.

(3) Similar the statement of (2).

Thm21 Hilbert's Basis theorem

If R is a Noetherian ring then so is polynomial ring $R[x]$.

Proof) Let I be an ideal of $R[x]$ and let $L_1 = \{ a \in R ; a x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in I \}$. Now, we check L_1 is an ideal of R.

Clearly, L_1 is nonempty. For $a, b \in L_1$ and $r \in R$, $\exists f(x), g(x) \in I$ with $f(x) = a \cdot x^n + \cdots$, $g(x) = b \cdot x^m + \cdots$. Since $x^m f(x), x^n \cdot g(x) \in I$ we have $(x^m f(x) - x^n g(x)) \in I$ and the coefficient of the leading term is $a - b$. Thus, $a - b \in L_1$, closed under subtraction and for $r \in R$, $a \in L_1 \Rightarrow ar \in L_1$ is obvious. Therefore L_1 is an ideal and since R is Noetherian, L_1 is finitely generated, for $a_1, \cdots a_n \in R$, $L_1 = (a_1, \cdots, a_n)$. Now for each $a_i \in L_1$ thus $\exists f_i(x) \in I$ with form $f_i(x) = a_i x^{n_i} + \cdots$ and let $N = \max \{ n_i ; 1 \le i \le n \}$.

For each $d \in \{ 0, \cdots, N-1 \}$ define $L_{id} := \{ a \in R ; a \cdot x^i + \cdots \in I ; i \le d \}$ and each L_{id} is an ideal of R. Since R is Noetherian, $\forall d \ \exists b_{d1}, b_{d2}, \cdots b_{dm_d}$, $L_{id} = (b_{d1}, b_{d2}, \cdots, b_{dm_d})$. Since for every $b_{di} \in L_{id}$, there exists $f_{di}(x) \in I$ with form $f_{di}(x) = b_{di} \cdot x^{d_i} + \cdots$.

Now let I' be an ideal generated by $\{ f_1(x), \cdots, f_n(x) \} \cup \{ f_{di}(x) ; 0 \le d \le N-1, 1 \le i \le m_d \}$ and we assert $I = I'$. $I' \subset I$ is clear. Suppose, $I \not\subset I'$, let $f(x) = a \cdot x^e + \cdots + a_0 \in I \setminus I'$ which has smallest degree in $I \setminus I'$.

If $e \ge N$. Since $a \in L_1 = (a_1, \cdots, a_n)$ we have $a = \sum_{1 \le i \le n} r_i a_i$ for some $r_i \in R$.

Then, $g(x) := r_1 x^{e-n_1} f_1(x) + r_2 x^{e-n_2} f_2(x) + \cdots + r_n x^{e-n_m} f_n(x) \in I' \subset I$ and also $f(x) - g(x) \in I$.

and $g(x)$ has the form $a \cdot x^c + \cdots$, so we have $f(x) - g(x) \in I'$ and since $g(x) \in I'$ we obtain $f(x) \in I'$, a contradiction.

If $c < N$. Since $f \in L_c$, f has the form $\sum_{1 \le i \le m_c} r_i \cdot b_{ci}$ where $r_1, \cdots, r_{m_c} \in R$.

Let $g(x) := \sum_{1 \le i \le m} r_i \cdot x^{c-d_i} f_{d_i} \in I'[x] \subset I[x]$ then we have $f(x) - g(x) \in I[x]$.

Now, $g(x)$ has the form $a \cdot x^c + \cdots$. Thus we have $\deg(f(x) - g(x)) < \deg(f(x))$ and $f(x) - g(x) \in I'[x]$ implies $f(x) \in I'[x]$. Therefore, $f(x) - g(x) \in I[x] \setminus I'[x]$, a contradiction.

Hence, we obtain $I[x] = I'[x]$, R is a Noetherian.

Cor 22. Every ideal in the polynomial ring $F[x_1, \cdots, x_n]$ with coefficients from a field F is finitely generated.

Thm 23 Fix a monomial ordering on $R = F[x_1, \cdots, x_n]$ and suppose $\{g_1, \cdots, g_m\}$ is a Gröbner basis for the nonzero ideal I in R. Then

(1) Every polynomial $f \in R$ can be written uniquely in the form $f = f_I + r$ where $f_I \in I$ and no nonzero monomial term of the 'remainder' r is divisible by any of the leading terms $LT(g_1), \cdots, LT(g_m)$.

(2) Both f_I and r can be computed by general polynomial division by $g_1, \cdots, g_m$ and are independent of the order in which these polynomials are used in the division.

(3) The remainder r provides a unique representative for the coset of f in the quotient ring $F[x_1, \cdots, x_n]/I$. In particular, $f \in I$ iff $r = 0$.

Proof). (1) By General Polynomial Division, for $f \in R$ there exists q_i and r such that $f = (q_1 g_1 + \cdots + q_m g_m) + r$ and let $f_I = q_1 g_1 + \cdots + q_m g_m$.

Suppose, $\exists f_I'$, r' with $f_I + r = f_I' + r'$ then $r - r' = f_I' - f_I \in I$ so, $LT(r-r') \in LT(I)$ $= (LT(g_1), \cdots, LT(g_m))$. Note that every element in $LT(I)$ has the form $\sum_{1 \le i \le m} f_i \cdot LT(g_i)$ with $f_i \in F[x_1, \cdots, x_n]$.

If $r \neq r'$, since r and r' are sum of monomial terms none of which divisible by any $LT(g_i)$, so is $r - r'$. This contradicts $r - r' \in (LT(g_1), \cdots, LT(g_m))$.

(2) We already seen the first assertion and the secound assertion is by (1).

(3) Since $f_I \in I$ we have $f \equiv r \bmod I$ and $f \in I$ iff $r = 0$ is obviously.

Prop 24 Fix a monomial on $R = F[x_1, \cdots, x_n]$ and let I be a nonzero ideal on R.

(1) If $g_1, \cdots, g_m$ are elements of I such that $LT(I) = (LT(g_1), \cdots, LT(g_m))$, then $\{g_1, \cdots, g_m\}$ is a Gröbner basis for I.

(2) The ideal I has a Gröbner basis.

Proof) (1) Let $g_1, \cdots, g_m \in I$ with $LT(I) = (LT(g_1), \cdots, LT(g_m))$.

It is enough to show that $I \subseteq (g_1, \cdots, g_m)$. For $f \in I$, by General Polynomial division, f has the form $\sum_{1 \le i \le m} q_i \cdot g_i + r$. Since $r = f - \sum_{1 \le i \le m} q_i g_i \in I$, we have $LT(r) \in LT(I) = (LT(g_1), \cdots, LT(g_m))$

If $r \neq 0$, $LT(r) \neq 0$, a contradiction. Hence we have $r = 0$, $f \in (g_1, \cdots, g_m)$.

(2) First we assert the following,

Let I be an ideal in $F[x_1, \cdots, x_n]$ generated by some set S. Then, a finite subset of S generates I.

By Cor 22. I is finitely generated, $I = (f_1, \cdots, f_m)$ for some $f_i \in F[x_1, \cdots, x_m]$.

For each i, since $f_i \in I = F[x_1, \cdots, x_n] \cdot S$ we have $f_i = \sum_{1 \le j \le m_i} g_{ij} \cdot s_{ij}$, $g_{ij} \in F[x_1, \cdots, x_n]$ and $s_{ij} \in S$ for every j

Then for $T = \{ s_{ij} ; 1 \le i \le m, 1 \le j \le m_i \}$ we have, $F[x_1, \cdots, x_m] S = F[x_1, \cdots, x_m] T$.

Now prove the assertion (2). Note that $LT(I) = (\{ LT(f) ; f \in I \})$. by previous assertion, $\exists h_1, \cdots, h_n \in I$, $LT(I) = (LT(h_1), \cdots, LT(h_n))$ and by (1) $\{ h_1, \cdots, h_n \}$ is a Gröbner basis.

Prop 1 The submodule Criterion

Let R be a ring and let M be an R-module. A subset N of M is a submodule of M iff

(1) $N \neq \emptyset$, and

(2) $x + ry \in N$ for all $r \in R$ and for all $x, y \in N$

Proof) ($\Rightarrow$) Obviously.

($\Leftarrow$) If N is a subgroup of M, obviously N is a R-submodule of M. Thus we verify N is a subgroup.

Since N is non-empty set, for all $n \in N$, on (ii) we pick r as (-1) then $n + (-n) = 0 \in N$ holds. Thus, N possesses an identity and an inverse $-n$ for all n and the associativity is manifestly holds.

Therefore, N is an R-submodule.

Prop 2 Let M, N and L be R-modules.

(1) A map $\varphi : M \to N$ is an R-module homomorphism iff $\varphi(rx + y) = r\varphi(x) + \varphi(y)$ for all $r \in R$ and all $x, y \in M$.

(2) Let φ, ψ be elements of $\mathrm{Hom}(M, N)$. Define $\varphi + \psi$ by

$$(\varphi + \psi)(m) = \varphi(m) + \psi(m) \quad \text{for all } m \in M$$

Then $\varphi + \psi \in \mathrm{Hom}(M, N)$ and with this operation $\mathrm{Hom}(M, N)$ is an Abelian

group. If R is commutative ring then for $r \in R$ define $r\varphi$ by

$$(r\varphi)(m) = r(\varphi(m)) \quad \text{for all } m \in M.$$

Then, $r\varphi \in \mathrm{Hom}(M,N)$ and with this action of the commutative ring R the Abelian group $\mathrm{Hom}(M,N)$ is an R-module.

(3) If $\varphi \in \mathrm{Hom}(M,N)$ and $\psi \in \mathrm{Hom}(M,N)$ then $\psi \circ \varphi \in \mathrm{Hom}(L,N)$

(4) With addition as above and multiplication defined as function composition, $\mathrm{Hom}(M,M)$ is a ring with 1. When R is commutative $\mathrm{Hom}(M,M)$ is an R-algebra.

Proof)

(1) Manifestly

(2) Let $r \in R$ and $n, m \in M$.

$$\begin{aligned}(\varphi+\psi)(rn+m) &= \varphi(rn+m) + \psi(rn+m) \\ &= r(\varphi(n)+\psi(n)) + \varphi(m) + \psi(m) \\ &= r((\varphi+\psi)(n)) + (\varphi+\psi)(n)\end{aligned}$$

Thus by (1), $\varphi+\psi \in \mathrm{Hom}(M,N)$.

We assert the function $0 : M \to N,\ m \mapsto 0$ for all m is an R-module homomorphism. Thus, clearly 0 is an identity of group $\mathrm{Hom}(M,N)$.

For all $\varphi \in \mathrm{Hom}(M,N)$, the inverse is a function which assign the m the $-\varphi(m)$ and an associative of low is obviously holds.

Thus, $\mathrm{Hom}(M,N)$ form a group.

Suppose R is a ring. For $r \in R$ and $\varphi \in \mathrm{Hom}(M,N)$.

$$(r\varphi)(nl+m) = r(\varphi(nl+m))$$

$$= r(n\varphi(l)+\varphi(m))$$

$$= n(r\varphi(l)+r\varphi(m))$$

$$= n((r\varphi)(l)+(r\varphi)(m)) \quad \text{for all } l \in R,\ n,m \in M.$$

Then by (1) $r\varphi \in \mathrm{Hom}(M,N)$.

Next we verify $\mathrm{Hom}(M,N)$ is an R-module over R.

Let $r, s \in R$ and $\varphi, \psi \in \mathrm{Hom}(M,N)$.

$$((r+s)\varphi)(m) = (r+s)(\varphi(m))$$

$$= r\cdot\varphi(m) + s\varphi(m)$$

$$= (r\varphi)(m) + (s\varphi)(m) \quad \text{for all } m$$

Thus, $(r+s)\varphi = r\varphi + s\varphi$.

$$((rs)\varphi)(m) = (rs)(\varphi(m))$$

$$= r\,s(\varphi(m))$$

$$= r(s\varphi)(m) \quad \text{for all } m$$

Thus, $(rs)\varphi = r(s\varphi)$.

$$(r(\varphi+\psi))(m) = r((\varphi+\psi)(m))$$

$$= r(\varphi(m)+\psi(m))$$

KOKUYO LOOSE-LEAF A-836BT 6 mm ruled×36 lines

$= r\varphi(m) + r\psi(m)$ for all m.

Thus, $r(\varphi+\psi) = r\varphi + r\psi$

for $1 \in R$,

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

$= \varphi(m)$ for all m

Thus, $1\cdot\varphi = \varphi$.

Therefore, $\mathrm{Hom}(M, N)$ is an R-module over R.

(3) For all $r \in R$ and $n, m \in L_1$.

$\psi\circ\varphi(rn+m) = \psi(r\varphi(n) + \varphi(m))$

$= r\,\psi(\varphi(n)) + \psi(\varphi(m))$

$= r\,(\psi\circ\varphi(n)) + (\psi\circ\varphi)(m)$

Then by (1), $\psi\circ\varphi \in \mathrm{Hom}(L_1, N)$

(4) It is easy to show $\mathrm{Hom}(M, M)$ is a ring with identity $1 : m \mapsto m$.

Suppose R is a commutative by (2) $\mathrm{Hom}(M, M)$ is an R-module. Let $f : R \to A$ be a function which assign the $r \in R$ the rI is a ring homomorphism and for all $\varphi \in \mathrm{Hom}(M, M)$ $(rI)(\varphi) = (\varphi)(rI)$ holds for all $r \in R$ thus, $f(R)$ is contained in the center of A.

Prop3 Let R be a ring, let M be an R-module and let N be a submodule of M. The additive quotient group M/N can be made into an R-module by defining an action of element of R by

$r(x+N) = (rx)+N$ for all $r \in R$ and $x \in M$

The natural projection map $\pi : M \to M/N$ defined by $\pi(x) = x+N$ is an R-module homomorphism with kernel N.

Proof). Since N is an R-submodule, N is normal, M/N is group and since M is an R-module, M/N is an Abelian group.

Let $r, s \in R$ and $x, y \in M$,

$$(r+s)((x+N)+(y+N)) = (r+s)((x+y)+N)$$
$$= (r+s)(x+y)+N$$
$$= (r(x+y)+N)+(s(x+y)+N),$$

$$(rs)(x+N) = (rsx)+N$$
$$= r(sx+N)$$

if R has an identity 1,

$$1(x+N) = (1 \cdot x)+N$$
$$= x+N$$

Therefore, M/N is an R-module over R.

Let $r \in R$ and $x, y \in M$

$$\pi(rx+y) = (rx+y)+N$$

$$= (rx)+N+y+N$$

$$= r\cdot(x+N)+y+N$$

$$= r\cdot\pi(x)+\pi(y).$$

Thus, by prop 2(i), π is an R-module homomorphism.

Finally we verify $N = \ker\varphi$

for all $n \in N$, $\pi(n) = n+N = 0+N$ thus, $N \subset \ker\varphi$

for all $x \in \ker\varphi$ then for all $y \in M$,

$\pi(x)+y+N = y+N$ thus, $x+N = N$, $x \in N$ hence $\ker\varphi \subset N$

Therefore, $N = \ker\varphi$

Thm 4 Isomorphism Theorems

(1) The First Isomorphism Theorem for Modules.

Let M, N be R-modules and let $\varphi: M \to N$ be an R-module homomorphism.

Then $\ker\varphi$ is a submodule of M and $M/\ker\varphi \cong \varphi(M)$.

(2) The Secound Isomorphism Theorem

Let A, B be submodules of the R-module M. Then $(A+B)/B \cong A/(A\cap B)$.

(3) The Third Isomorphism Theorem

Let M be an R-module, and let A and B be submodules of M with $A \subseteq B$.

Then $(M/A)/(B/A) \approx M/B$.

④ The Fourth or Lattice Isomorphism Theorem

Let N be a submodule of the R-module M. There is a bijection between the submodule of M which contain N and the submodule of M/N. The correspodence is given by $A \leftrightarrow A/N$, for all $A \supseteq N$. This correspondence commutes with the processes of taking sums and intersection.

Proof)

(1) For all $r \in R$ and $x, y \in \ker \varphi$,

$$\varphi(rx+y) = r\varphi(x) + \varphi(y)$$

$$= r \cdot 0 + 0$$

$$= 0$$

thus, $rx+y \in \ker \varphi$, $\ker \varphi$ is a submodule of M.

Now, it is clear that $n+N = m+N$ implies $\varphi(n) = \varphi(m)$. Thus we can defined a function as $\psi : n+N \mapsto \varphi(n)$.

We verify ψ is an R-module homomorphism.

For all $r \in R$ and $n, m \in N$,

$$\psi(r(n+\ker\varphi) + (m+\ker\varphi)) = \psi((rn+m)+\ker\varphi)$$

$$= \varphi(rn+m)$$

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

Thus, φ is an R-module homomorphism.

Suppose $\varphi(n)=\varphi(m)$ holds, then, $\varphi(n-m)=0$, $n-m\in\ker\varphi$

thus, $n+\ker\varphi=m+\ker\varphi$, φ is injective and the surjection is manifestly.

Therefore, $M/\ker\varphi\approx\varphi(M)$.

(2) Let $\varphi: A\to(A+B)/B\ ;\ a\mapsto a+B$ then obviously φ is an R-module homomorphism.

For all $a\in A$ and $b\in B$, $(a+b)+B=a+B$ then φ is surjective.

Next we verify $\ker\varphi=A\cap B$.

$\forall x\in\ker\varphi$, $\varphi(x)=x+B=0+B$ holds, then $x\in B$ and by definition of φ, $x\in A$

thus, $\ker\varphi\subset A\cap B$.

$\forall x\in A\cap B$, $\varphi(x)=x+B=0+B$ thus, $x\in\ker\varphi$, $A\cap B\subset\ker\varphi$

Therefore by (1), $(A+B)/B\approx A/(A\cap B)$

(3) Since, $n+A=m+A$ implies $n+B=m+B$ holds, we can define a function φ as

$\varphi: M/A\to M/B\ ;\ n+A\mapsto n+B$.

and this function φ is manifestly surjective. Thus, it is enough to show that $\ker\varphi=B/A$.

For all $b\in B$, $\varphi(b+A)=b+B=0+B$ thus, $b+A\in\ker\varphi$, $B/A\subset\ker\varphi$.

For all $x+A\in\ker\varphi$. $\varphi(x+A)=x+B=0+B$ then, $x\in B$ thus, $\ker\varphi\subset B/A$

Therefore by (1) $(M/A)/(B/A)\approx M/B$.

(4) Now we can pick a function φ as statement (not necessarily bijective)

Suppose $A+N = B+N$ holds.

For all $a \in A$ there exists $b \in B$ and $n \in N$ such that $a = b+n \in B$.

Thus, $A \subset B$. Similary $B \subset A$. Then, $A = B$, φ is injective.

Let L/N be a submodule of M/N

for all $r \in R$ and $s,t \in L$

$$(rs+t)+N = r(s+N)+(t+N)$$
$$\in L/N.$$

thus for some $l \in L$ and $n \in N$, $rs+t = l+n \in L$.

Hence, by prop 1 L is a submodule of M, φ is surjective.

Next we verify

(i) $\varphi(A \cap B) = \varphi(A) \cap \varphi(B)$

(ii) $\varphi(A+B) = \varphi(A) + \varphi(B)$

(i) (c) $\forall x \in A \cap B$, $x \in A$ and $x \in B$ holds thus, $\varphi(x) \in \varphi(A) \cap \varphi(B)$.

$\varphi(A \cap B) \subset \varphi(A) \cap \varphi(B)$

(⊃) $\forall z \in \varphi(A) \cap \varphi(B)$ $\exists a, b \in A, B$, $z = \varphi(a) = \varphi(b)$ thus, $\varphi(a-b) = 0$

Then for some $n \in N$, $a = b+n \in B$, $a \in A \cap B$.

Therefore $\varphi(A) \cap \varphi(B) \subset \varphi(A \cap B)$

(ii) (c) $\forall a \in A, b \in B$, $\varphi(a) \in \varphi(A)$ and $\varphi(b) \in \varphi(B)$.

thus, $\varphi(a+b) = \varphi(a) + \varphi(b) \in \varphi(A) + \varphi(B)$. Hence, $\varphi(A+B) \subset \varphi(A) + \varphi(B)$.

(b) $\forall z \in \varphi(A) + \varphi(B)$ $\exists a, b \in A, B$ $z = \varphi(a) + \varphi(b)$.

$$\begin{aligned} z &= \varphi(a) + \varphi(b) \\ &= \varphi(a+b) \\ &\in \varphi(A+B) \end{aligned}$$

thus, $\varphi(A) + \varphi(B) \subset \varphi(A+B)$

Prop5 Let $N_1, N_2, \cdots, N_k$ be submodules of the R-module M. Then the following are equivalent.

(1) The map $\pi : N_1 \times N_2 \times \cdots \times N_k \to N_1 + N_2 + \cdots + N_k$ defined by

$$\pi(a_1, a_2, \cdots, a_k) = a_1 + a_2 + \cdots + a_k$$

is an isomorphism of R modules : $N_1 + N_2 + \cdots + N_k \cong N_1 \times N_2 \times \cdots \times N_k$.

(2) $N_j \cap (N_1 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k) = 0$ for all $j \in \{1, \cdots, k\}$.

(3) Every $x \in N_1 + \cdots + N_k$ can be written uniquely in the form $a_1 + a_2 + \cdots + a_k$ with $a_i \in N_i$.

Proof) (1) $\Rightarrow$ (2)

For every x in $N_1 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k$ with the form $x = x_1 + \cdots + x_{j-1} + x_{j+1} + \cdots + x_k$, $x + 0$ is also an element of $N_1 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k$. Now by assumption, there exists unique $\vec{0}$ such that $\pi(\vec{0}) = 0$ and obviously, $\pi(x_1, \cdots, x_{j-1}, 0, x_{j+1}, \cdots x_k) = \vec{0}$ holds.

Hence, the j-th element of 0 is equals to 0 this assert (2).

(2) $\Rightarrow$ (3)

Suppose there exists some $x \in N_1 + \cdots + N_k$ such that x can written in a different form such that

$$x = a_1 + \cdots + a_k = b_1 + \cdots + b_k, \quad a_j \neq b_j \text{ for some } j.$$

Now, $a_j - b_j = (a_1 - b_1) + \cdots + (a_{j-1} - b_{j-1}) + (a_{j+1} - b_{j-1}) + \cdots + (a_k - b_k)$ holds.

By assumption, if above equations holds, it equals to 0. This contradicts $a_j \neq b_j$.

(3) $\Rightarrow$ (1)

Obviously π is bijective. Thus we verify π is an R-module homomorphism.

Let $r \in R$ and $(a_1, \cdots, a_k), (b_1, \cdots, b_k) \in N_1 + \cdots + N_k$

$$\pi\big(r(a_1, \cdots, a_k) + (b_1, \cdots, b_k)\big) = \pi\big((ra_1 + b_1) + \cdots + \pi(ra_k + b_k)\big)$$

$$= (ra_1 + b_1) + \cdots + (ra_k + b_k)$$

$$= r(a_1 + \cdots + a_k) + (b_1 + \cdots + b_k)$$

$$= r\pi(a_1, \cdots, a_k) + \pi(b_1, \cdots, b_k)$$

Then, π is an R-module isomorphism.

Thm 6 For any set A there is a free R-module $F(A)$ on the set A and $F(A)$ satisfies the following universal propety : if M is any R-module and $\varphi : A \to M$ is any map of sets, then there is a unique R-module homomorphism $\Phi : F(A) \to M$ such that $\Phi(a) = \varphi(a)$, for all $a \in A$, that is TFAE,

$$\begin{array}{ccc} A & \longrightarrow & F(A) \\ & \searrow^{\varphi} & \downarrow \Phi \\ & & M \end{array}$$

When A is the finite set $\{a_1, \cdots, a_n\}$, $F(A) = Ra_1 \oplus \cdots \oplus Ra_n \approx R^n$.

Proof). If $A = \{\}$, let $F(A) = \{0\}$ then the statement holds.

Suppose $A \neq \{\}$, let $F(A) = \{f : A \to R \;;\; f(a) = 0$ for all but finitely many $a \in A\}$, define an addition and an action as follow;

for all $f, g \in F(A)$ and $r \in R$,

$$f + g := a \mapsto f(a) + g(a),$$

$$rf := a \mapsto r f(a).$$

In this sense $F(A)$ is an R-module over R.

Now, we identifing set A as subset of $F(A)$, the collection of function $a \mapsto f_a$ for all a and $f_a : A \to R \;;\; a \mapsto 1,\ a \neq b \mapsto 0$. Then obviously, every element of $F(A)$ written by R-combination of A such that $r_1 a_1 + r_2 a_2 + \cdots + r_n a_n$ moreover, this representation is unique.

Let $\varphi : A \to M$ a map, M is an R-module, define the function Ψ by

$$\sum_{1 \le i \le n} r_i a_i \mapsto \sum_{1 \le i \le n} r_i \cdot \varphi(a_i).$$

We verify Ψ is an R-module homomorphism.

Let $\sum_{1 \le i \le n} r_i a_i$, $\sum_{1 \le i \le m} l_i b_i \in F(A)$ and $r \in R$ and $r_{n+i} := l_i$, $a_{n+i} := b_i$ for $1 \le i \le m$.

Then,

$$\Psi\left(r\left(\sum_{1 \le i \le n} r_i a_i\right) + \sum_{1 \le i \le m} l_i b_i\right) = \Psi\left(\sum_{1 \le i \le n} r r_i a_i + \sum_{n+1 \le i \le m+n} r_i a_i\right)$$

$$= \sum_{1 \le i \le n} r r_i \Psi(a_i) + \sum_{n+1 \le i \le m+n} r_i \Psi(a_i)$$

$$= r\left(\sum_{1\le i\le n} r_i\,\varphi(a_i)\right) + \sum_{1\le i\le m} d_i\,b_i$$

$$= r\varphi\left(\sum_{1\le i\le n} r_i\,a_i\right) + \varphi\left(\sum_{1\le i\le n} d_i\,b_i\right)$$

Hence, φ is an R-module homomorphism and the uniqueness is obvious.

Finally, suppose that A is finite.

Since, for every $a_i \in A$, $\{a_i\}$ is a submodule of $F(A)$, prop 5 (3) assert, $F(A) = Ra_1 \oplus \cdots \oplus Ra_1$ and since $Ra_i \approx R$ for every $a_i \in A$, $F(A) \approx R^n$.

Cor 7

(1) If F_1 and F_2 are free modules on the same set A, there is a unique isomorphism between F_1 and F_2 which is the identity map on A.

(2) If F is any free R-module with basis A, then $F \approx F(A)$. In paticular, F enjoys the same universal propety with respect to A as $F(A)$ does in Thm 6.

Proof).

(1) Define a function $\varphi : F_1 \to F_2$ by $\sum_{1\le i\le n} r_i\,a_i \mapsto \sum_{1\le i\le n} r_i\,a_i$ then φ is isomorphism.

(2) By (1), $F \approx F(A)$ and F has the universal propety.

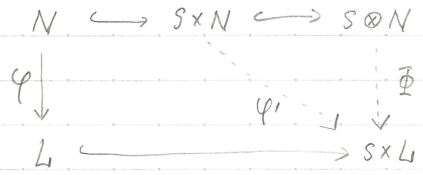
Thm 8. Let R be a subring of S, let N be a left R-module and let $\iota : N \to S \otimes N$ be the R-module homomorphism defined by $\iota(n) = 1 \otimes n$. Suppose that L is any left S-module (hence also an R-module) and that $\psi : N \to L$ is an R-module homomorphism from N to L. Then there is a unique S-module homomorphism $\Phi : S \otimes N \to L$ such that ψ factors through Φ, i.e., $\psi = \Phi \circ \iota$. Conversely, if $\Phi : S \otimes N \to L$ is an S-module homomorphism then $\psi = \Phi \circ \iota$ is an R-module homomorphism from N to L.

KOKUYO LOOSE-LEAF ノ-836BT 6 mm ruled×36 lines

No.

Date

Proof). Immediately by the following diagram. Note that φ' is S-bilinear map.



Cor 9. Let $\iota : N \to S \otimes N$ be the R-module homomorphism in Theorem 8. Then $N/\ker\iota$ is the unique largest quotient of N that can be embedded in any S-module. In paticular, N can be embedded as an R-submodule of some left S-module iff ι is injective.

Thm10 Suppose R is a ring with 1, M is a right R-module, and N is a left R-module. Let $M \otimes_R N$ be the tensor product of M and N over R and let $\varphi : M \times N \to M \otimes_R N$ be the R-balanced map defined above.

(1) If $\Phi : M \otimes_R N \to L$ is any group homomorphism from $M \otimes_R N$ to an Abelian group L then the composite map $\psi = \Phi \circ \varphi$ is an R-balanced map from $M \times N$ to L.

(2) Conversely, suppose L is an Abelian group and $\psi : M \times N \to L$ is any R-balanced map. Then there exists a unique group homomorphism $\Phi : M \otimes_R N \to L$ such that ψ factors through φ.

Proof).

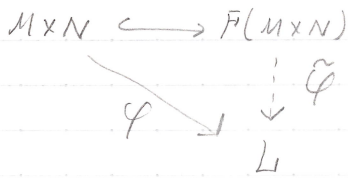
(1) We verify ψ is R-balanced.

$$\begin{aligned}\psi(m_1 + m_2, n) &= \Phi(\varphi(m_1 + m_2, n)) \\ &= \Phi(\varphi(m_1, n), \varphi(m_2, n)) \\ &= \Phi\varphi(m_1, n) + \Phi\varphi(m_2, n) \\ &= \psi(m_1, n) + \psi(m_2, n)\end{aligned}$$

Similarly, $\psi(m, n_1 + n_2) = \psi(m, n_1) + \psi(m, n_2)$.

$$\begin{aligned}\psi(mr, n) &= \Phi\varphi(mr, n) \\ &= \Phi\varphi(m, rn) \\ &= \psi(m, rn)\end{aligned}$$

(2) By Thm 6. there exists unique $\tilde{\psi}$ with free R-module $F(M \times N)$.



Now, we assert $H \leq \ker \tilde{\varphi}$ with $M \otimes N = F(M \times N)/H$

$$\tilde{\varphi}((m_1+m_2, n) - (m_1, n) - (m_2, n)) = \tilde{\varphi}(m_1+m_2, n) - \tilde{\varphi}(m_1, n) - \tilde{\varphi}(m_2, n)$$

$$= \varphi(m_1+m_2, n) - \varphi(m_1, n) - \varphi(m_2, n)$$

$$= 0$$

Similarly, $\tilde{\varphi}((m, n_1+n_2) - (m, n_1) - (m, n_2)) = 0$

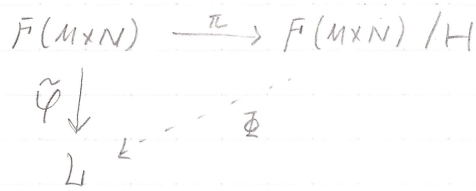
$$\tilde{\varphi}((m, rn) - (mr, n)) = \tilde{\varphi}(m, rn) - \tilde{\varphi}(mr, n)$$

$$= \varphi(m, rn) - \varphi(mr, n)$$

$$= 0$$

Then, every generator of H is in $\ker \tilde{\varphi}$ i.e. $H \leq \ker \tilde{\varphi}$

Hence by homomorphism property TFAE.



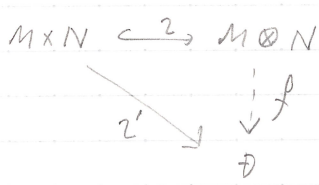
Cor 11 Suppose D is an Abelian group and $\varphi' : M \times N \to D$ is an R-balanced map such that

(i) The image of φ' generates D as an Abelian group, and

(ii) Every R-balanced map defined on $M \times N$ factors through φ' as in Thm 10.

Then there is an isomorphism $f: M \otimes_R N \approx D$ of Abelian groups with $z' = f \circ z$.

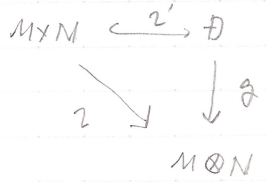
Proof). By Thm 10 (2) there exists unique group homomorphism such that TFDC



First we show f is surjective. By (i) for every $d \in z(M \times N)$ we can pick (m,n) as $z'(m,n) = d$. moreover, $f(z(n.m)) = d$ holds.

And since every element of $M \otimes N$ has the form $\sum_{\text{finite}} m \otimes n$, f is a surjection.

Next we show f is injective. By (ii) there exists g such that TFDC



Then, $z = (g \circ f) \circ z$ thus, for every (m,n), $m \otimes n = z(m,n) = (g \circ f)\, z$.

Moreover, $\sum_{\text{finite}} m \otimes n = \sum_{\text{finite}} (g \circ f)(m \otimes n)$

this assert $g \circ f = id$, f is injective

Cor 12 Suppose R is a commutative ring. Let M and N be two left R-modules and let $M \otimes_R N$ be the tensor product of M and N over R, where M is given the standared R-module structure.

Then $M \otimes_R N$ is a left R-module with

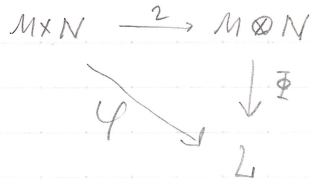
$$r(m \otimes n) = rm \otimes n = (mr) \otimes n = m \otimes rn,$$

KOKUYO LOOSE-LEAF A-80ERT 6 mm RULED A5B 7mm

and the map $\iota : M \times N \to M \otimes_R N$ with $\iota(m,n) = m \otimes n$ is an R-bilinear map. If L is any left R-module then there is a bijection

$$\{R\text{-bilinear maps } : M \times N \to L\} \longleftrightarrow \{R\text{-module homomorphism } M \otimes N \to L\}$$

where the correspondence between φ and Φ is given by the commutative diagram.



Proof) First we assert $M \otimes N$ is an R-module. Define an action by $s \cdot \sum_{\text{finite}} m \otimes n := \sum_{\text{finite}} (sm) \otimes n$ $= \sum_{\text{finite}} m \otimes (ns)$. We verify this action is well-defined.

First we show for every $s \in R$, $\varphi : M \times N \longrightarrow M \otimes N$; $(m,n) \longmapsto m \otimes n$ is R-balanced.

$$\varphi(m_1 + m_2, n) = (m_1 + m_2) \otimes n$$

$$= m_1 \otimes n + m_2 \otimes n$$

$$= \varphi(m_1, n) + \varphi(m_2, n).$$

Similarly $\varphi(m, n_1 + n_2) = \varphi(m, n_1) + \varphi(m, n_2)$

$$\varphi(m, rn) = m \otimes rn$$

$$= mr \otimes n$$

$$= r\,\varphi(m,n)$$

Thus, φ is R-balanced then by Thm 10(2) there exists unique group homomorphism

$$M\times N \xrightarrow{\iota} M\otimes N$$
$$\varphi \searrow \quad \downarrow \lambda_s$$
$$M\otimes N$$

And, $\sum_{\text{finite}} (sm\otimes n) = \sum_{\text{finite}} \lambda_s (sm\otimes n) = \lambda_s \sum_{\text{finite}} m\otimes n$

Thus, an action $\left(s, \sum_{\text{finite}} m\otimes n\right) \mapsto \sum_{\text{finite}} sm\otimes n$ is well-defined.

Next, we verify, ι is R-bilinear

$$\iota(r_1m_1 + r_2m_2, n) = (r_1m_1 + r_2m_2)\otimes n$$
$$= (r_1m_1)\otimes n + (r_2m_2)\otimes n$$
$$= r_1(m_1\otimes n) + r_2(m_2\otimes n)$$
$$= r_1\,\iota(m_1,n) + r_2\cdot\iota(m_2,n)$$

$$\iota(m, r_1n_1 + r_2n_2) = m\otimes(r_1n_1 + r_2n_2)$$
$$= m\otimes r_1n_1 + m\otimes r_2n_2$$
$$= r_1\,\iota(m_1,n_1) + r_2\cdot\iota(m_1,n_2).$$

Next we show there exists bicorrespondence.

Let L be an R-module, $\varphi: M\times N \to L$ be R-bilinear moreover, φ is R-balanced.

Then by Thm 10(2) there exists unique group homomorphism Φ such that $T\,F\,D\,C$

$$M\times N \xrightarrow{\iota} M\otimes N$$
$$\varphi \searrow \quad \downarrow \Phi$$
$$L$$

Since, $\Phi(r(m\otimes n)) = \Phi((rm)\otimes n) = \varphi(rm,n) = r\varphi(m,n) = r\Phi(m,n)$ and Φ is addtive thus, Φ is R-module homomorphism.

And, the assignment $\varphi \mapsto \Phi$ is obviously injective.

We assert this assertment is surjective.

It is enough to show for R-module homomorphism Φ, $\Phi\circ\iota$ is R- bilinear map.

$$\Phi\circ\iota(r_1m_1+r_2m_2, n) = \Phi(r_1(\iota(m_1,n)) + r_2(\iota(m_2,n)))$$

$$= r_1\Phi\iota(m_1,n) + r_2\Phi\iota(m_2,n)$$

$$\Phi\circ\iota(m, r_1n_1+r_2n_2) = \Phi(r_1\cdot\iota(m,n_1)+r_2\cdot\iota(m,n_2))$$

$$= r_1\Phi\iota(m,n_1)+r_2\Phi\iota(m,n_2).$$

Thus, the assignment is surjective, there exists bijection.

Thm13. The "Tensor Product" of Two Homomorphisms.

Let M, M' be right R-modules, let N, N' be left R-modules, and suppose $\varphi: M\to M'$ and $\psi: N\to N'$ are R-module homomorphisms.

(1) There is a unique group homomorphism, denoted by $\varphi\otimes\psi$, mapping $M\otimes_R N$ into $M'\otimes N'$ such that $(\varphi\otimes\psi)(m\otimes n) = \varphi(m)\otimes\psi(n)$ for all $m\in M$ and $n\in N$.

(2) If M, M' are also (S,R)-bimodules for some ring S and φ is also an S-module homomorphism, then $\varphi\otimes\psi$ is a homomorphism of left S-modules. In paticular, if R is commutative then $\varphi\otimes\psi$ is always an R-module homomorphism for the standard R-module structure.

(3) If $\lambda : M' \to M''$ and $\mu : N' \to N''$ are R-module homomorphisms then

$$(\lambda \otimes \mu) \circ (\varphi \otimes \psi) = (\lambda \circ \varphi) \otimes (\mu \circ \psi).$$

Proof)

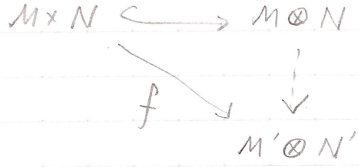
We show that a map $f : M \times N \to M' \otimes N'$ which assign the (m,n) the $\varphi m \otimes \psi n$ is an R-balanced map.

$$\begin{aligned} f(m_1+m_2, n) &= \varphi(m_1+m_2) \otimes \psi n \\ &= (\varphi(m_1) + \varphi(m_2)) \otimes \psi n \\ &= \varphi m_1 \otimes \psi n + \varphi m_2 \otimes \psi n \\ &= f(m_1, n) + f(m_2, n) \end{aligned}$$

Similarly $f(m, n_1+n_2) = f(m, n_1) + f(m, n_2)$.

$$\begin{aligned} f(mr, n) &= \varphi(mr) \otimes \psi n \\ &= \varphi(m) r \otimes \psi n \\ &= \varphi m \otimes \psi(rn) \\ &= f(m, rn). \end{aligned}$$

Thus, by Thm 10 there exists unique group homomorphism such that TFAE.



(2) Since M (resp. M') is an (S,R)-bimodule and N (resp. N') is a left R-module, $M \otimes N$

(resp. $M' \otimes N'$) is an S- module. ($s \sum n \otimes m := \sum sn \otimes m$)

We show the following assertion

$$(\varphi \otimes \psi)(s(m \otimes n)) = s \cdot (\varphi \otimes \psi)(m \otimes n)$$

(LSH) $= (\varphi \otimes \psi)(sm \otimes n)$

$= \varphi(sm) \otimes \psi n$

$= s\,\varphi(m) \otimes \psi n$

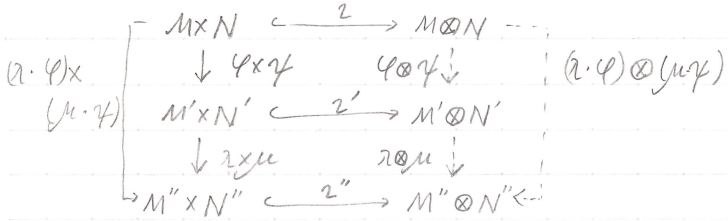
$= s(\varphi m \otimes \psi n)$

$= s(\varphi \otimes \psi)(m \otimes n)$

$= (RSH)$

And by (1), $\varphi \otimes \psi$ is an S- module homomorphism. In paticular, if R is commutative, we obtain a right R- module then, M is an $(R\text{-}R)$- bimodule, thus, $\varphi \otimes \psi$ is an R-module homomorphism.

(3) Manifestly by TFDC



Thm 14 Associativity of the Tensor Product.

Suppose M is a right- R module, N is an (R, T)- bimodule, and L is a left T- module. Then there exists a unique isomorphism $(M \otimes_R N) \otimes_T L \cong M \otimes_R (N \otimes_T L)$ of Abelian groups such

that $(m\otimes n)\otimes l \longmapsto m\otimes(n\otimes l)$. If M is an (S,R)- bimodule, then this is an isomorphism of S-modules.

Proof) Fixed $l\in L$, define a map $\varphi: M\to N\to M\otimes(N\otimes L);\ (m,n)\longmapsto m\otimes(n\otimes l)$, we show φ is R-balanced.

$$\varphi(m_1+m_2,\ n) = (m_1+m_2)\otimes(n\otimes l)$$
$$= m_1\otimes(n\otimes l)+m_2\otimes(n\otimes l)$$
$$= \varphi(m_1,n)+\varphi(m_2,l)$$

$$\varphi(m,\ n_1+n_2) = m\otimes\left((n_1+n_2)\otimes l\right)$$
$$= m\otimes\left(n_1\otimes l+n_2\otimes l\right)$$
$$= m\otimes(n_1\otimes l)+m\otimes(n_2\otimes l)$$
$$= \varphi(m,n_1)+\varphi(m,n_2)$$

$$\varphi(m,rn) = m\otimes(rn\otimes l)$$
$$= m\otimes(r(n\otimes l))$$
$$= mr\otimes(n\otimes l)$$
$$= \varphi(mr,n)$$

Thus, φ is an R-balanced, by Thm 10 there exists unique Φ

$$\begin{array}{ccc} M\times N & \hookrightarrow & M\otimes N \\ & \searrow^{\varphi} & \downarrow \Phi \\ & & M\otimes(N\otimes L) \end{array}$$

Next, we define

$\Psi : (M \otimes N) \times L \longrightarrow M \otimes (N \otimes L)\,;\ (m \otimes n, \ell) \mapsto m \otimes (n \otimes \ell)$

We easy to verify Ψ is a T-balaced.

If M is an (S, R)-bimodule, since, $M \otimes (N \otimes L)$ is an S-module, $(M \otimes N) \otimes L$ in an S-module.

We have only show that $\tilde{\Phi}'$ is homogeneous.

$$\tilde{\Phi}'\left(s((m \otimes n) \otimes \ell)\right) = \tilde{\Phi}'\left(s(m \otimes n) \otimes \ell\right)$$

$$= \tilde{\Phi}'\left((sm \otimes n) \otimes \ell\right)$$

$$= sm \otimes (n \otimes \ell)$$

$$= s(m \otimes (n \otimes \ell))$$

$$= s\,\tilde{\Phi}'\left((m \otimes n) \otimes \ell\right).$$

Therefore we have the result.

Cor15 Suppose R is commutative and M, N, and L are left R-modules. Then $(M \otimes N) \otimes L \simeq M \otimes (N \otimes L)$ as R-modules for the statdard R-module structures M, N and N.

Proof) Since M, N and L are (R, R)-bimodule manifestly holds by previous theorem.

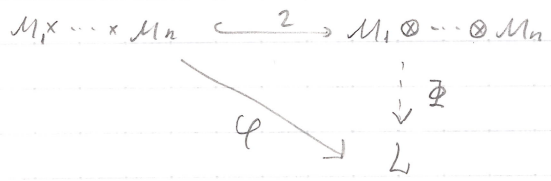
Cor16 Let R be a commutative ring and let $M_1, \cdots, M_n, L$ be R-modules. Let $M_1 \otimes \cdots \otimes M_n$ denote any bracketing of the tensor product of these modules and let $\tau : M_1 \times \cdots \times M_n \longrightarrow M_1 \otimes \cdots \otimes M_n$ be the map defined by $\tau(m_1, \cdots, m_n) = m_1 \otimes \cdots \otimes m_n$. Then

(1) for every R-module homomorphism $\Phi : M_1 \otimes \cdots \otimes M_n \to L$ the map $\varphi = \Phi \circ \iota$ is n-multilinear from $M_1 \times \cdots \times M_n$ to L, and

(2) if $\varphi : M_1 \times \cdots \times M_n \to L$ is an n-multilinear map then there is a unique R-homomorphism $\Phi : M_1 \otimes \cdots \otimes M_n \to L$ such that $\varphi = \Phi \circ \iota$. Hence there is a bijection

$\{ n\text{-multilinear maps } \varphi : M_1 \times \cdots \times M_n \to L \} \leftrightarrow \{ R\text{-module homomorphism } \Phi : M_1 \otimes \cdots \otimes M_n \to L \}$

with respect to which TFDC.



Proof) (1)

$$\varphi(m_1, \cdots, m_{i-1}, r \cdot m_i + r' \cdot m_i', m_{i+1}, \cdots, m_n)$$

$$= \Phi(m_1 \otimes \cdots \otimes m_{i-1} \otimes (r \cdot m_i + r' m_i') \otimes m_{i+1} \otimes \cdots \otimes m_n)$$

$$= \Phi(m_1 \otimes \cdots \otimes m_{i-1} \otimes r m_i \otimes m_{i+1} \otimes \cdots \otimes m_n) + \Phi(m_1 \otimes \cdots \otimes m_{i-1} \otimes r' m_i' \otimes m_{i+1} \otimes \cdots \otimes m_n)$$

$$= \Phi((r m_1) \otimes \cdots \otimes m_{i-1} \otimes m_i \otimes m_{i+1} \otimes \cdots \otimes m_n) + \Phi((r' m_1) \otimes \cdots \otimes m_{i-1} \otimes m_i' \otimes m_{i+1} \otimes \cdots \otimes m_n)$$

$$= \Phi(r(m_1 \otimes \cdots \otimes m_i \otimes \cdots \otimes m_n)) + \Phi(r'(m_1 \otimes \cdots \otimes m_i' \otimes \cdots \otimes m_n))$$

$$= r\,\Phi(m_1 \otimes \cdots \otimes m_i \otimes \cdots \otimes m_n) + r'\,\Phi(m_1 \otimes \cdots \otimes m_i' \otimes \cdots \otimes m_n)$$

$$= r \cdot \varphi(m_1, \cdots, m_i, \cdots, m_n) + r' \varphi(m_1, \cdots, m_i', \cdots m_n).$$

Thus, φ is n-multilinear.

(2) Mimic the proof of cor 12

Thm 17. (Tensor products of Direct Sums.)

Let M, M' be right R-modules and let N, N' be left R-modules. Then there are unique group isomorphisms

$$(M \oplus M') \otimes N \simeq (M \otimes N) \oplus (M' \otimes N),$$

$$M \otimes (N \oplus N') \simeq (M \otimes N) \oplus (M' \otimes N).$$

such that $(m, m') \otimes n \mapsto (m \otimes n, m' \otimes n)$ and $m \otimes (n, n') \mapsto (m \otimes n, m \otimes n')$ respectively.

If M, M' are also (S, R)-bimodules, then these are isomorphisms of left S-modules.

In particular, if R is commutative, these are isomorphism of R-modules.

Proof) Let φ be a map from $(M \oplus M') \times N$ into $(M \otimes N) \times (M' \otimes N)$ which assign the $(m, m') \otimes n$ the $(m \otimes n, m \otimes n')$, then φ is R-balanced.

By universal propety there is a unique group homomorphism as TFAE.

$$\begin{array}{ccc} (M \oplus M') \times N & \hookrightarrow & (M \oplus M') \otimes N \\ & \searrow^{\varphi} & \downarrow \Phi \\ & & (M \otimes N) \oplus (M' \otimes N) \end{array}$$

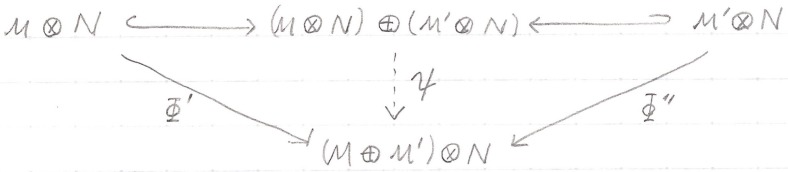
Next, we define the maps f and g by

$$f : M \times N \longrightarrow (M \oplus M') \otimes N \;;\; (m, n) \longmapsto (m, 0) \otimes n$$

$$g : M' \times N \longrightarrow (M \oplus M') \otimes N \;;\; (m', n) \longmapsto (0, m') \otimes n$$

then, clearly f and g are R-balanced. Thus, by universal propety there exists Φ' and Φ'' such that TFAE.

Thus, there exists unique Ψ as TFDC



Now, we assert $\Phi \circ \Psi$, $\Psi \circ \Phi$ are identity maps.

Thus, $(M \otimes N) \oplus (M' \otimes N) \simeq (M \oplus M') \otimes N$ holds.

Similarly, $(M \otimes N) \oplus (M \otimes N') \simeq M \otimes (N \oplus N')$ holds.

Futher, if R is commutative, then M and M' are regarded as (R, R)-bimodule, so we have the result.

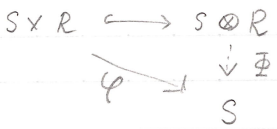
Cor 18 Extension of Scalars for Free Modules.

The module obtained from the free R-module $N \simeq R^n$ by extension of scalars from R to S is the free S-module S^n, i.e., $S \otimes R^n \simeq S^n$ as left S-module.

Proof)

By previous theorem, $S \otimes N \simeq S \otimes R^n = (S \otimes R)^n$ holds. So it is enough to show that $S \otimes R \simeq S$ as S-modules.

For a function $\varphi : S \times R \to S \; ; \; (s, r) \mapsto sr$, since φ is R-balanced, by universal propety there exists unique group homomorphism Φ as TFDC



Now, $\Phi\left(s'(s\otimes r)\right) = \Phi\left((s's)\otimes r\right) = s'\Phi(s\otimes r)$ holds, Φ is left R-module homomorphism.

And for $\Phi' : S \to S\otimes R\ ;\ s \mapsto s\otimes 1$ obviously $\Phi'\circ\Phi$, $\Phi\circ\Phi$ are identity map.

Therefore $S\otimes N \simeq S^n$

Cor19. Let R be a commutative ring and let $M \simeq R^s$ and $N \simeq R^t$ be free R-modules with bases $m_1, \cdots, m_s$ and $n_1, \cdots, n_t$, respectively. Then $M\otimes N$ is a free R-module of rank st, with basis $m_i\otimes n_j$, $1\le i\le s$ and $1\le j\le t$ i.e., $R^s\otimes R^t \simeq R^{st}$.

Proof). By Thm 17 clearly holds.

Prop20 Suppose R is a commutative ring and M, N are left R-modules, considered with the standard R-module structures. Then there is a unique R-module $M\otimes N \simeq N\otimes M$ mapping $m\otimes n$ to $n\otimes m$.

Proof). Since the function $\varphi : M\times N \to N\otimes M\ ;\ (m,n) \mapsto n\otimes m$ is R-balanced, by universal propety obviously $M\otimes N \simeq N\otimes M$ holds.

Prop21. Let R be a commutative ring and let A and B be R-algebras. Then the multiplication $(a\otimes b)(a'\otimes b') = aa'\otimes bb'$ is well defined and makes $A\otimes B$ into an R-algebra.

Proof) Let φ be the map $A\times B\times A\times B \to A\otimes B\ ;\ (a,b,a',b') \mapsto (aa')\otimes(bb')$.

Then since,

$$\varphi(r_1a_1+r_2a_2, b, a', b') = \left((r_1a_1+r_2a_2)a'\right)\otimes(bb')$$

$$= \left((r_1a_1)a' + (r_2a_2)a'\right)\otimes(b\cdot b')$$

NB See 10.4, 10.5

Date

$$= (r_1(a_1 a') + r_2(a_2 a')) \otimes (b b')$$

$$= (r_1(a a')) \otimes (b b') + (r_2 (a_2 a')) \otimes (b b')$$

$$= (r_1((a_1 a') \otimes (b b')) + (r_2 (a_2 a') \otimes (b b'))$$

$$= r_1 \varphi(a_1, b, a', b') + r_2 \varphi(a_2, b, a' b')$$

Thus, φ is multilinear over R, then by Cor16, there exists R-module homomorphism as TFAE

$$\begin{array}{ccc} A \times B \times A \times B & \longrightarrow & A \otimes B \otimes A \otimes B \\ & \searrow^{\varphi} & \downarrow \Phi \\ & & A \otimes B \end{array}$$

And we can obtain a bilinear map ψ as TFAE

$$\begin{array}{ccc} (A \otimes B) \times (A \otimes B) & \longrightarrow & (A \otimes B) \otimes (A \otimes B) \\ & \searrow^{\psi} & \downarrow \Phi \\ & & A \otimes B \end{array}$$

Now, we show that $A \otimes B$ is an R-algebra.

Since ψ is bilinear and A and B are rings, $A \otimes B$ is a ring with an identity $1_A \otimes 1_B$.

Let $h : R \to A \otimes B ; r \mapsto f(r) \otimes 1_B$ where f is a function induced by an R-algebra A. Then clearly $h = i \circ f$ and clearly i and f are ring homomorphism, then so is h. And, $h(R) \subset Z(A \otimes B)$ will be easily proven. □

Prop 22. Let A, B and C be R-modules over some ring R. Then

(1) The sequence $0 \longrightarrow A \xrightarrow{\psi} B$ is exact iff ψ is injective.

(2) The sequence $B \xrightarrow{\varphi} C \longrightarrow 0$ is exact iff φ is surjective.

KOKUYO LOOSE-LEAF A-836ST 6 mm ruled 26 lines

Proof) Obvious.

Cor 23. The sequence $0 \to A \xrightarrow{\psi} B \xrightarrow{\varphi} C \to 0$ is exact iff ψ is injective, φ is surjective, and $\operatorname{im}\psi = \ker\varphi$ i.e. B is extension of C by A.

Proof) Manifestly by previous theorem.

Prop 24 The short Five lemma

Let α, β, γ be a homomorphism of short exact sequences.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow\alpha & & \downarrow\beta & & \downarrow\gamma & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

(1) If α and γ are injective, then so is β.

(2) If α and γ are surjective then so is β.

(3) If α and γ are isomorphism then so is β (and then the two sequences are isomorphic).

Proof)

(1) It is enough to show that $\beta(b) = 0$ implies $b = 0$ for all $b \in B$ ($\because$ β is homomorphism).

Let $b \in B$ with $\beta(b) = 0$. Then $\varphi'(\beta(b)) = 0 = \gamma(\varphi(b))$.

Since γ is injective, $\varphi(b) = 0$, so, $b \in \ker\varphi = \operatorname{im}\psi$. Thus for some $a \in A$, $\psi(a) = b$, $0 = \beta(b) = \beta\psi(a) = \psi'\alpha(a)$.

Since, ψ' and α are injective, $a = 0$, $\psi(a) = 0$. Thus, $b = 0$.

(2) For $b' \in B'$, since γ, φ are surjective, $\exists b \in B$ $\varphi'(b') = \gamma(\varphi(b)) = \varphi'(\beta(b))$.

Thus, $\varphi'(b' - \beta(b)) = 0$, $b' - \beta(b) \in \ker \varphi' = \operatorname{im} \psi'$.

$\exists a \in A$, $b' - \beta(b) = \psi' \alpha(a) = \beta\psi(a)$.

$b' = \beta(b) + \beta\psi(a) = \beta(b + \psi(a))$

Thus, β is surjective.

(3) By (1) and (2) manifestly.

Prop 25. The short exact sequence $0 \to A \xrightarrow{\psi} B \xrightarrow{\varphi} C \to 0$ of R-modules is split iff if there is an R-module homomorphism $\mu : C \to B$ such that $\varphi \circ \mu$ is the identity map on C. Similarly, the short exact sequence $1 \to A \xrightarrow{\psi} B \xrightarrow{\varphi} C \to 1$ of groups is split iff there is a group homomorphism $\mu : C \to B$ such that $\varphi \circ \mu$ is the identity map on C.

Proof). Let B be a split. Since $A \oplus C \approx \psi(A) \oplus C$ let $\mu : A \oplus C \to A ; (\psi(a), c) \mapsto a$

Prop27. Let D, L_1 and M be R-modules and let $\psi : L_1 \to M$ be an R-module homomorphism. Then the map $\psi' : \mathrm{Hom}(D, L_1) \to \mathrm{Hom}(D, M) ; f \mapsto \psi \circ f$ is a homomorphism of Abelian groups. If ψ is injective, then ψ' is also injective, i.e., if $0 \to L_1 \xrightarrow{\psi} M$ is exact, then $0 \to \mathrm{Hom}(D, L_1) \xrightarrow{\psi'} \mathrm{Hom}(D, M)$ is also exact.

Proof) For $f, g \in \mathrm{Hom}(D, L_1)$,

$$\psi'(f+g) = \psi(f+g) = \psi f + \psi g = \psi'(f) + \psi'(g).$$

Thus, ψ' is homomorphism of Abelian groups.

Next, suppose ψ is injective. if $\psi'(f) = \psi'(g)$ then $\psi f = \psi g$. Since ψ is injective, $f = g$. Thus, ψ' is injective.

Thm28 Let D, L_1, M and N be R-modules. If $0 \to L_1 \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0$ is exact, then the associated sequence $0 \to \mathrm{Hom}(D, L_1) \xrightarrow{\psi'} \mathrm{Hom}(D, M) \xrightarrow{\varphi'} \mathrm{Hom}(D, N)$ is exact. ---(10.10)

A homomorphism $f : D \to N$ lifts to a homomorphism $\bar{f} : D \to M$ iff $f \in \mathrm{Hom}(D, N)$ is in the image of φ'. In general $\varphi' : \mathrm{Hom}(D, M) \to \mathrm{Hom}(D, N)$ need not be surjective; the map φ' is surjective iff every homomorphism from D to N lifts to a homomorphism from D to M, in which case the sequence (10) can be extented to a short exact sequence.

The sequence (10) is exact for all R-modules D iff the sequence $0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} N$ is exact.

Proof) First we verify (10) is exact. Since ψ' is injective and φ' is surjective, it is enough to show that $\mathrm{im}\,\psi' = \ker \varphi'$.

Let $\bar{F} \in \operatorname{im} \Psi'$ then there exists $F' \in \mathrm{Hom}(D, L)$ such that $\bar{F} = \Psi \cdot F'$.

Then, $\Phi'(\bar{F}) = \Phi \cdot (\Psi \cdot F') = 0$. Hence $\bar{F} \in \ker \Phi'$, $\operatorname{im} \Psi' \subseteq \ker \Phi'$.

Let $\bar{F} \in \ker \Psi'$ then $\Psi'(\bar{F}) = 0$ holds. Since $\operatorname{im} \Psi' = \ker \Phi'$, for every $d \in D$, $\Phi(\bar{F}(d)) = 0$ implies $\bar{F}(d) \in \operatorname{im} \Psi$. Now, for $\bar{F}(d) = \Psi(n)$, $\Psi'(d \mapsto n) = (d \mapsto \Psi n)$ $= (d \mapsto \bar{F} d) = \bar{F}$. This assert $\bar{F} \in \operatorname{im} \Psi'$, $\ker \Phi \subseteq \operatorname{im} \Psi'$.

Therefore, $\operatorname{im} \Psi' = \ker \Phi'$, (10) is exact.

The next assertion, Φ' is sujective iff every arrow in $\mathrm{Hom}(D, N)$ lifts to an arrow in $\mathrm{Hom}(D, M)$ not necessarily uniquely exists, is manifestly.

We verify last assertion, (10) is exact for all R-modules D iff $0 \to L \xrightarrow{\Psi} M \xrightarrow{\Phi} N$ is exacts.

($\Leftarrow$) Clear.

($\Rightarrow$) First we show that $R(R, X)$ is R-module and then show that $R(R, X) \simeq X$ as R-module for every R-module X. Define an action of R on $R(R, X)$ by $r \cdot f : R \to X ; r' \mapsto f(r \cdot r')$ then $R(R, X)$ form an R-module.

Next, we define a map, $\Phi_X : R(R, X) \to X ; f \mapsto f(1)$. Then, $\Phi_X(rf + g) = (rf + g)(1) =$ $(rf)(1) + g(1) = f(r) + g(1) = r \cdot f(1) + g(1)$ holds, Φ_X is an R-module homomorphism from $R(R, X)$ into X.

Next let Φ'_X be an R-module homomorphism X into $R(R, X)$ which assign the x the $\varphi_x : r \mapsto rx$

Then, $(\Phi'_X \circ \Phi_X)(f) = \Phi'_X(f(1)) = \varphi_{f(1)} = (r \mapsto f(r)) = f$,

$(\Phi_X \circ \Phi'_X)(x) = \Phi_X(\varphi_x) = \varphi_x(1) = x$.

Therefore, Φ_X is an R-module isomorphism. $R(R,X) \approx X$ as R-module.

This asserts TFAE,

$$\begin{array}{ccccccccc} 0 & \longrightarrow & R(R,L) & \xrightarrow{\mathcal{F}'} & R(R,M) & \xrightarrow{\mathcal{G}'} & R(R,N) & \longrightarrow & 0 \\ & & \Phi_L \downarrow\downarrow & & \Phi_M \downarrow\downarrow & & \Phi_N \downarrow\downarrow & & \\ 0 & \longrightarrow & L & \xrightarrow{\mathcal{F}} & M & \xrightarrow{\mathcal{G}} & N & \longrightarrow & 0 \end{array} .$$

This diagram asserts, $0 \to L \xrightarrow{\mathcal{F}} M \xrightarrow{\mathcal{G}} N \to 0$ is exact.

Prop 29. Let D, L and N be R-modules. Then

(1) $R(D, L \oplus N) \approx R(D,L) \oplus R(D,N)$, and

(2) $R(L \oplus N, D) \approx R(L,D) \oplus R(N,D)$.

Proof).

(1) Define $\Phi : R(D, L\oplus N) \to R(D,L) \oplus R(D,N)$; $f \longmapsto (p_1 f, p_2 f)$. Then, Φ is group homomorphism.

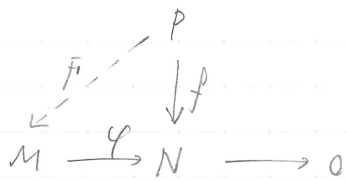
Define, $\Phi' : R(D,L) \oplus R(D,N) \to R(D, L\oplus N)$; $(f_1, f_2) \mapsto f : d \mapsto (f_1 d, f_2 d)$. Then Φ' is a group homomorphism.

And easy to check $\Phi' \circ \Phi$ and $\Phi \circ \Phi'$ are identies. Thus, $R(D, L\oplus N) \approx R(D,L) \oplus R(D,N)$

Prop 30 Let P be an R-module. Then the following are equivalent:

(1) For any R-modules L, M and N, if $0 \to L \xrightarrow{\mathcal{F}} M \xrightarrow{\mathcal{G}} N \to 0$ is a short exact sequence then $0 \to R(P,L) \xrightarrow{\mathcal{F}'} R(P,M) \xrightarrow{\mathcal{G}'} R(P,N) \to 0$ is also a short exact sequence.

(2) For any R-modules M and N if $M \xrightarrow{\varphi} N \to 0$ is exact, then every R-module homomorphism from P into N lifts to an R-module homomorphism into M, i.e. given $f \in R(P, N)$ there is a lift $F \in R(P, M)$ making TFDC:



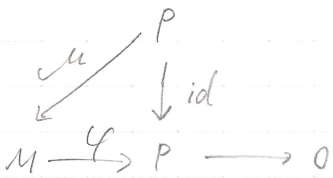
(3) If P is a quotient of the R-module M then P is isomorphic to a direct summand of M, i.e. every short exact sequence $0 \to L \to M \to P \to 0$ splits.

(4) P is a directed summand of a free R-module.

Proof). By prop 28 (1) $\Leftrightarrow$ (2) holds, thus we show (2) $\Rightarrow$ (3) $\Rightarrow$ (4) $\Rightarrow$ (2).

(2) $\Rightarrow$ (3).

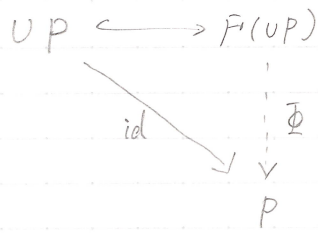
Let $0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} P \to 0$ be exact. By assumption there is a μ as TFDC:



This assert there exists μ such that $\mu \circ \varphi = id$ by prop 25. the exact sequence is split.

(3) $\Rightarrow$ (4)

By universal propety of free module, there exists R-module homomorphism Φ such that TFDC:



moreover, Φ is epi. We obtain the following exact sequence, $0 \to \ker\Phi \hookrightarrow F'(UP) \xrightarrow{\Phi} P \to 0$.

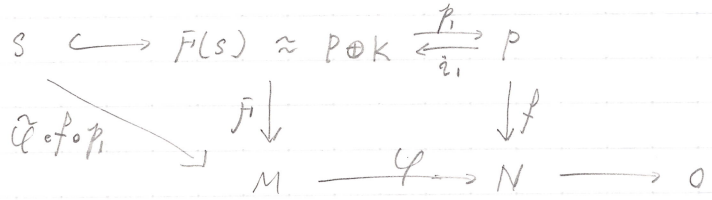
By assumption $F'(UP) \approx \ker\Phi \oplus P$ so, P is direct summand of a free module $F'(UP)$.

(4) $\Rightarrow$ (2)

Let $F'(S) = P \oplus K$ where S is a set, K is an R-module and let $M \xrightarrow{\varphi} N \xrightarrow{\psi} 0$ be an exact sequence.

For $f \in Hom(P, N)$, let $p_1 : F'(S) \to P$ be a natural projection and $n_S := f \circ p_1 \in Hom(F'(S), N)$.

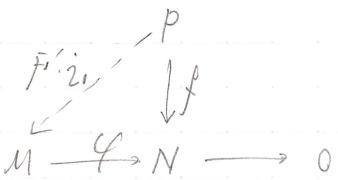
Now, since ψ is surjective, assuming Axiom of choice there exists $\tilde{\psi}$ such that $\tilde{\psi}\psi = id$. Then $\tilde{\psi} \cdot f \cdot p_1 : S \to M$ (not nessesarily $\tilde{\psi}$, $\tilde{\psi} \circ f \circ p_1$ are R-module homomorphism) and there exists unique F' as TFAC:



Now for every $s \in S$, $\psi F'(s) = \psi(\tilde{\psi} f p_1(s)) = f p_1(s)$ holds. $\psi F' = f p_1$ as a map, hence the above diagram commutes.

Moreover, since $p_1 \cdot i_1 = id$, $\psi F' \cdot i_1 = f$ holds. This asserts TFAC.

KOKUYO LOOSE-LEAF ... RIGHT ...



And the uniqueness propety is obvious.

Cor 3.1. Free modules are projective. A finitely generated module is projective iff it is a direct summand of a finitly generated free module. Every module is a quotient of a projective module.

Proof) The first assertion is immediately for every free module F, $F \simeq F \oplus \cdots$.

Next we prove the next assertion, let F be a finitely generated module with finite set P. Then $\bar{\Phi} : \bar{F}(P) \simeq \bar{F}$ holds. Moreover, $0 \to \ker \bar{\Phi} \to \bar{F}(P) \xrightarrow{\bar{\Phi}} \bar{F} \to 0$ is exact.

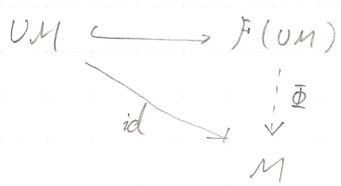
Since $\bar{F}$ is projective, the exact sequence is splits, $F(P) \simeq \ker \bar{\Phi} \oplus F$.

Thus, F is direct summand of finitely generated free module.

Conversely is by (4) $\Rightarrow$ (1) in previous proposition.

Finally, we show that every R-module M is a quotient of a projective module.

For, UM, as a set, there exists Φ as TFDC



and, moreover, since $\bar{\Phi}$ is surjective, $F(M)/\ker\Phi \simeq M$.

Now, (1) assert $F(M)$ is projective. Thus, we complete the proof.

Cor 32. If D is an R-module, then the functor $\mathrm{Hom}(D, -)$ from the category of R-modules to the category of Abelian groups is left exact. It is exact iff D is a projective R-module.

Proof) Obviously by thm 28.

Thm 33 Let D, L, M and N be R-modules. If $0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0$ is exact, then the associated sequence $0 \to R(N,D) \xrightarrow{\varphi'} R(M,D) \xrightarrow{\psi'} R(L,D)$ is exact. ... (10.12)

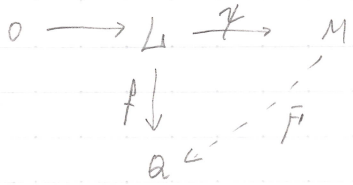
A homomorphism $f: L \to D$ lifts to a homomorphism $\bar{f}: M \to D$ iff $f \in R(L,D)$ is in the image of ψ'. In general $\psi': R(M,D) \to R(L,D)$ need not be surjective; the map ψ' is surjective iff every homomorphism from L to D lifts to a homomorphism from M to D, in which case the sequence (12) can be extended to a short exact sequence. The sequence (12) is exact for all R-modules D iff the sequence $L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0$ is exact.

Proof). See thm 28 and proved by obvious dual manner.

Prop 34 Let Q be an R-module. Then the following are equivalent:

(1) For any R-modules L, M and N, if $0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0$ is a short exact sequence, then $0 \to R(N,Q) \to R(M,Q) \to R(L,Q) \to 0$ is also a short exact sequence.

(2) For any R-modules L and M, if $0 \to L \xrightarrow{\psi} M$ is exact, then every R-module homomorphism from L into Q lifts to an R-module homomorphism of M into Q, i.e. given $f \in R(L,Q)$ there is a lift $\bar{f} \in R(M,Q)$ making $\triangle FDC$



(3) If Q is a submodule of the R-module M then Q is a direct summand of M, i.e., every short exact sequence $0 \to Q \to M \to N \to 0$ splits.

Proof) See prop 30 and proved by obvious dual manner.

Cor35 If D is an R-module, then the functor $R(-, D)$ from the category of R-modules to the category of Abelian group is left exact. It is exact iff D is an injective R-module.

Proof) See cor 32 and proved by obvious dual manner.

Prop36. Let Q be an R-module.

(1) Baer's Criterion. The module Q is injective iff for every left ideal I of R any R-module homomorphism $g: I \to Q$ can be extended to an R-module homomorphism $G: R \to Q$.

(2) If R is a P.I.D. then Q is injective iff $rQ = Q$ for every nonzero $r \in R$. In paticular, a $\mathbb{Z}$-module is injective iff it is divisible. When R is a P.I.D., quotient modules of injective R-modules are again injective.

Proof)

(1) ($\Rightarrow$) Easy.

($\Leftarrow$) Let $0 \to L \xrightarrow{\gamma} M$ be exact and let $f \in \mathrm{Hom}(L, Q)$. Define

$$S := \{ (f', L') : f'|_L = f \text{ and } L' \text{ is a submodule of } M \text{ with } L' \supseteq L = \gamma(L) \}$$

Note that S is not a void set.

Define an order $\leq$ on S by $(f_1, L_{i1}) \leq (f_2, L_{i2})$ if $f_2|_{L_{i1}} = f_1$ and $L_{i1} \subseteq L_{i2}$ then S is a poset. Let $\mathcal{A} = \{(f_i, L_i) ; i \in I\}$ be a chain of S. Then $\cup \mathcal{A}$ is a submodule of M including L_i.

Define $\tilde{f} : \cup L_i \to Q ; x \mapsto f_i(x)$ and let $U := (\tilde{f}, \cup L_i)$.

To show that U is an upper bound of $\mathcal{A}$ in S.

Let $(f_i, L_i) \in \mathcal{A}$. Then $\tilde{f}|_{L_i} = f_i$ and $L_i \subseteq \cup L_i$ this assert $\mathcal{A}$ has an upper bound U. Then by Zorn's lemma S has a maximal element (F, M').

Now we assert $M' = M$.

Suppose $M' \neq M$, let $m \in M \setminus M'$ and let $I := \{r \in R ; rm \in M'\}$, we show I is a left ideal.

Let $a, b \in I$ and $r \in R$.

(i) Verify $a - b \in I$.

Since $am, bm \in M'$, $am - bm \in M'$ thus $a - b \in I$.

(ii) Verify $ra \in I$

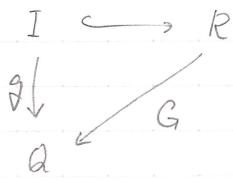
Since $am \in M'$ and $r(am) \in M'$, thus $(ra)m \in M'$ and $ra \in I$.

Hence I is a left ideal of R.

Define a map $g : I \to Q ; x \mapsto F(x, m)$.

Since $g(ra+b) = r\,g(a) + g(b)$ holds $g \in \mathrm{Hom}(I, Q)$.

By assumption there exists G such that TFDC



Since M' is a submodule of M, so is $M' + Rm$, and $M' + Rm \supsetneq M'$.

Now define a function $F' : M' + Rm \longrightarrow Q$, first we show the following:

$$m_1' + r_1 m = m_2' + r_2 m \text{ implies } F'(m_1') + G(r_1) = F'(m_2') + G(r_2) \quad \cdots (*)$$

For $m_1' + r_1 m = m_2' + r_2 m$,

$$(r_1 - r_2)m = (m_1' - m_2') \in M' \text{ so } (r_1 - r_2) \in I$$

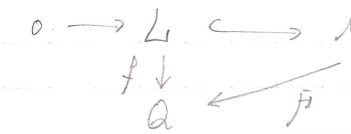
$$G(r_1) - G(r_2) = G(r_1 - r_2) = g(r_1 - r_2) = F((r_1 - r_2)m) = F(r_1 m - r_2 m)$$

$$= F(m_2' - m_1') = F(m_2') - F(m_1')$$

Thus, (*) holds, we obtain a function which assign the $m' + rm$ the $F(m') + G(r)$.

Futher, $F'(r'(m_1' + r_1 m) + (m_2' + r_2 m)) = r' F'(m_1' + r_1 m) + F'(m_2' + r_2 m)$ holds. Hence $F' \in \mathrm{Hom}(M' + Rm, Q)$ and moreover $F'|_{M'} = F$.

Thus, $(F, M') \leq (F', M' + Rm)$ holds. This assert $(F, M') = (F', M' + Rm)$, $M' = M' + Rm$. This contradicts $M' \subsetneq M' + Rm$. Thus $M' = M$ and TFDC:



(2)

($\Rightarrow$) It is enough to show that $\forall r \in R \setminus \{0\}$, $rQ \subset Q$.

Let $q \in Q$ and $r \in R \setminus \{0\}$.

Define $f : Rr \longrightarrow Q \; ; sr \longmapsto s \cdot q$. Since $f(r'(s_1 r) + (s_2 r)) = r' f(s_1 r) + f(s_2 r)$,

$f \in \mathrm{Hom}(Rr, Q)$.

Since, Q is injective, by Baer's Criterion theorem there exists F such that $F|_{Rr} = f$.

$$\begin{array}{ccc} Rr & \hookrightarrow & R \\ {\scriptstyle f}\downarrow & \swarrow_{F} & \\ Q & & \end{array}$$

Now, $q = f(1 \cdot r) = F(r) = r \cdot F(1) \in r \cdot Q$. Thus, $Q \subseteq rQ$.

($\Leftarrow$) Suppose for all $r \in R \setminus \{0\}$, $rQ \subset Q$.

Let I be non-zero left ideal of R and let $f \in \mathrm{Hom}(I, Q)$.

Since R is P.I.D. for some non-zero x, $I = (x) = Rx$.

By assumption, there exists some q such that $f(x) = xq$.

Define a map $F : R \to Q \; ; r \longmapsto rq$ then clearly $F \in \mathrm{Hom}(R, Q)$.

To verify $F|_I = f$. Let $\gamma \in I$ then there exists $r \in R$ such that $\gamma = r \cdot x$ thus,

$$F(\gamma) = \gamma \cdot q = rx \cdot q = f(r \cdot x) = f(\gamma).$$

Therefore by Baer's Criterion, Q is injective.

The second assertion is obviously by previous assertion.

Next we verify the third assertion.

Let Q be injection and let K be a submodule of Q. Let $r \in R \setminus \{0\}$ and let $q+K \in Q/K$.

Then there exists $q' \in Q$ such that $q = r \cdot q'$.

So, $q+K = rq'+K = r(q'+K) \in r+Q/K$. Thus, $Q/K \subseteq r \cdot Q/K$ and moreover

$Q/K = r \cdot Q/K$.

Therefore by first assertion Q/K is injective.

Thm39. Suppose that D is a right R-module and that L, M and N are left modules. If $0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0$ is exact, then the associated sequence of abelian groups

$D \otimes L \xrightarrow{1 \otimes \psi} D \otimes M \xrightarrow{1 \otimes \varphi} D \otimes N \to 0$ is exact ... (10.13)

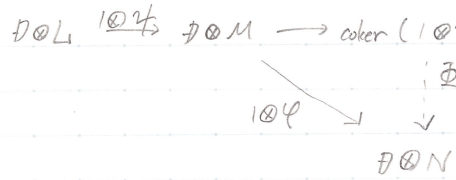
If D is an (S,R)-bimodule then (13) is an exact sequence of left S-modules. In paticular, if $S = R$ is a commutative ring, then (13) is an exact sequence of R-modules with respect to the standared R-module structures. The map $1 \otimes \varphi$ is not in general injective, i.e., the sequence (13) cannot in general be extended to a short exact sequence.

The sequence (13) is exact for all right R-modules D iff $L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0$ is exact.

Proof) First, we show that (13) is exact, i.e., $\operatorname{im}(1 \otimes \psi) = \ker(1 \otimes \varphi)$.

($\subseteq$) It suffice to show $(1 \otimes \varphi)(1 \otimes \psi) = 0$. For arbitrary $d \otimes l \in D \otimes L$, since $\varphi \psi = 0$, we obtain $(1 \otimes \varphi)(1 \otimes \psi)(d \otimes l) = 0$.

(2) Let $\bar{\varphi}$ be a group morphism as follows:



Since ψ is epi, define a function $\pi : D \times N \to \operatorname{coker}(1\otimes\psi) = D\otimes M/\operatorname{im}(1\otimes\psi)$ which assign the (d,n) the $d\otimes m$ with $\varphi(m)=n$. This function is well-defined because $\varphi(m-m')=0$ implies $m-m' \in \operatorname{im}(1\otimes\psi)$ and clearly π is R-balanced so there exists a morphism $\Phi' : D\otimes N \to \operatorname{coker}(1\otimes\psi)$.

Since, Φ is surjective, uniquely exists, $\Phi\circ\Phi' = id$ and by definition, $\Phi'\circ\Phi = id$.

Therefore, $\operatorname{coker}(1\otimes\psi) = 1\otimes\varphi = \operatorname{coim}(1\otimes\varphi)$

Finally, suppose that if (13) is exact for every right R-module D. Set $D=R$, then since $R\otimes X \cong X$ for arbitrary right modules X. We immediately complete the proof.

Prop 40. Let A be a right R-module. Then the following are equivalent :

(1) For any left R-modules L, M, and N, if $0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0$ is a short exact sequence, then $0 \to A\otimes L \xrightarrow{1\otimes\psi} A\otimes M \xrightarrow{1\otimes\varphi} A\otimes N \to 0$ is also a short exact sequence.

(2) For any left R-modules L and M, if $0 \to L \xrightarrow{\psi} M$ is an exact sequence of left R-modules then $0 \to A\otimes L \xrightarrow{1\otimes\psi} A\otimes M$ is an exact sequence of Abelian groups.

Proof) Immediate from thm 39.

Prop 41 If D is a right R-module, then the functor $D\otimes-$ from the category of left R-modules to the category of Abelian groups is right exact. If D is an (S,R)-bimodule, then $D\otimes-$ is a right exact functor from the category of left R-modules to the category of left S-modules. The functor is exact iff D is a Flat R-module

KOKUYO LOOSE-LEAF A-868BT 6 mm ruled x 36 lines

Proof) Derived from thm 39 and the definition of flat module.

Cor42. Free modules are flat; more generally, projective modules are flat.

Proof). To show that the free R-module F is flat it suffices to show that for any injective R-modules homomorphism $\psi: L \to M$ the induced map $1 \otimes \psi: F \otimes L \to F \otimes M$ is also injective.

First, we think of the case for finite generated free module, R^n. Since we have $R^n \otimes N = \oplus (R \otimes N) = N^n$, $R^n \otimes M = M^n$. Thus the isomorphism $id \otimes \psi: R^n \otimes N \to R^n \otimes M$ is injective.

Now, we prove the general case. Let A be a set and $F(A)$ the free module endowed with A. Suppose $(1 \otimes \psi)(f \otimes n) = 0$ for $f \otimes n \in F(A) \otimes N$. Since, f has the form $f = \sum_{1 \le i \le n} r_i a_i$ where $r_i \in R$ and $a_i \in A$ for each i, let $A' := \{a_i ; 1 \le i \le n\}$ then we have $f \in F(A')$ and $F(A') \hookrightarrow F(A)$. So we can identifing $f \otimes n \in F(A) \otimes N$ with $f \otimes n \in F(A') \otimes N \hookrightarrow F(A) \otimes N$.

Therefore, the morphism $1 \otimes \psi: F(A') \otimes N \to F(A') \otimes M$ is injective, moreover, $1 \otimes \psi: F(A) \otimes N \to F(A) \otimes M$ is injective since we have $F(A) \hookrightarrow F(A')$.

Finally, we verify the general case. Since, P is a projective module, there exists module P' such that $F = P \oplus P'$ is free. For an injection $\psi: N \to M$ we already have $1 \otimes \psi: F \otimes N \to F \otimes M$ is injective and since we have $F \otimes N = (P \otimes N) \oplus (P' \otimes N)$ and $F \otimes M = (P \otimes M) \oplus (P' \otimes M)$, $1 \otimes \psi: P \otimes N \to P \otimes M$ also injective.

Thm43. Adjoint Associativity.

Let R and S be rings, let A be a right R-module, let B be an $(R\text{-}S)$ module and let C be a right S-module. Then there is an isomorphism of Abelian groups $\mathrm{Hom}_S(A \otimes_R B, C) \simeq \mathrm{Hom}_R(A, \mathrm{Hom}_S(B, C))$.

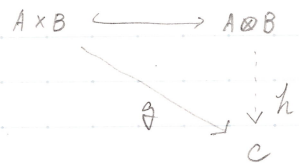
If $R = S$ is commutative this is an isomorphism of R-modules with the standard R-module structures.

Proof) Note that $A \otimes B$ is a right S-module by $(a \otimes b) \cdot s = a \otimes (b \cdot s)$ and $\mathrm{Hom}(B, C)$ is a right R-module by $\varphi \cdot r = (b \mapsto \varphi(rb))$.

First, for $\varphi \in \mathrm{Hom}(A \otimes B, C)$ and $a \in A$ define $\Phi(a) : B \to C \; ; \; b \mapsto \varphi(a \otimes b)$ then $\Phi(a)$ is an S-module homomorphism and moreover, Φ is an R-module homomorphism, i.e., $\Phi \in \mathrm{Hom}(A, \mathrm{Hom}(B, C))$. Now we assert the function α which assign the $\varphi \in \mathrm{Hom}(A \otimes B, C)$ the Φ which defined in above is a group homomorphism.

Let $\varphi, \varphi' \in \mathrm{Hom}(A \otimes B, C)$ then for $a \in A$ and $b \in B$, $\alpha(\varphi + \varphi')(a)(b) = (\varphi + \varphi')(a \otimes b) = \varphi(a \otimes b) + \varphi'(a \otimes b) = \alpha(\varphi)(a)(b) + \alpha(\varphi')(a)(b)$. So, $\alpha(\varphi + \varphi')(a) = \alpha(\varphi)(a) + \alpha(\varphi)(a)$ moreover, $\alpha(\varphi + \varphi') = \alpha(\varphi) + \alpha(\varphi')$.

Second, for $f \in \mathrm{Hom}(A, \mathrm{Hom}(B, C))$ define $\vartheta : A \times B \to C \; ; \; (a, b) \mapsto f(a)(b)$ then since ϑ is an R-balanced map there exists the morphism as follows :



which assign the $a \otimes b$ the $\vartheta(a, b)$.

Similarly, we obtain a group homomorphism $\beta : \mathrm{Hom}(A, \mathrm{Hom}(B, C)) \to \mathrm{Hom}(A \otimes B, C) \; ; \; f \mapsto h$. And immediately, we have $\alpha \circ \beta = id$ and $\beta \circ \alpha = id$.

The second assertion is clear.

Cor 4.4 If R is commutative then the tensor product of two projective R-modules is projective.

KOKUYO LOOSE-LEAF

Proof) Let P_1 and P_2 be projective R-modules and let $M \xrightarrow{\varphi} N \to 0$ be exact sequence. Since, P_2 is projective and R is commutative, and P_1 is projective, we obtain the following exact sequence:

$$\mathrm{Hom}(P_1, \mathrm{Hom}(P_2, M)) \xrightarrow{(\varphi_*)_*} \mathrm{Hom}(P_1, \mathrm{Hom}(P_2, N)) \to 0,$$

and by thm 43 we have $\mathrm{Hom}(P_1 \otimes P_2, M) \xrightarrow{\varphi'} \mathrm{Hom}(P_1 \otimes P_2, N) \to 0$ is exact. Note that by the proof of thm43, φ' is a morphism which assign the γ the $\varphi\gamma$. Therefore, $P_1 \otimes P_2$ is projective.

Prop 1 Assume the set $\mathcal{A} = \{v_1, \cdots, v_n\}$ spans the vector space V but no proper subset of $\mathcal{A}$ spans V. Then $\mathcal{A}$ is a basis of V. In paticular, any finitely generated vector space over F is a free F-module.

Proof) For $a_1, \cdots, a_n \in F$ with $a_1 v_1 + \cdots + a_n v_n = 0$, suppose for some i, $a_i \neq 0$. Let $a_1 \neq 0$ w.l.o.g., then we have $v_1 = -\left(\frac{a_2}{a_1} v_2 + \cdots + \frac{a_n}{a_1} v_n\right)$ this assert $\{v_2, \cdots, v_n\}$ spans V, a contradiction. The "paticular" assertion is manifestly since vectorspace is module.

Cor 2. Assume the finite set $\mathcal{A}$ spans the vector spaces V. Then $\mathcal{A}$ contains a basis of V.

Proof) Let $\mathcal{B}$ be subset of $\mathcal{A}$ such that $\mathcal{B}$ spans V and every proper subset of $\mathcal{B}$ not spans V. Then, by prop 1 clearly $\mathcal{B}$ is a basis.

Thm 3. A Replacement Theorem.

Assume $\mathcal{A} = \{a_1, \cdots, a_n\}$ is a basis for V containing n elements and $\{b_1, \cdots, b_m\}$ is a set of linearly independent vectors in V. Then there exists ordering $a_1, \cdots, a_n$ such that for each $k \in \{1, \cdots, m\}$ the set $\{b_1, \cdots, b_k, a_{k+1}, \cdots, a_n\}$ is a basis of V. In other words, the elements $b_1, \cdots, b_m$ can be used to successively replace the elements of the basis $\mathcal{A}$, still retaining a basis.

In paticular, $n \geq m$.

Proof) Proved by induction on k. If $k = 0$, manifestly. Les $k \geq 1$. Suppose that $\{b_1, \cdots, b_k, a_{k+1}, \cdots, a_n\}$ is a basis. Then since $b_{k+1} \in V = \text{span}\{b_1, \cdots, b_k, a_{k+1}, \cdots, a_n\}$, $\exists \beta_1, \cdots, \beta_k, \alpha_{k+1}, \cdots, \alpha_n \in F$,

$\beta_1 b_1 + \cdots + \beta_k b_k + \alpha_{k+1} a_{k+1} + \cdots + \alpha_n a_n = b_{k+1}$ ····· (*)

Now, not all α_i is zero thus, by reordering we have $\alpha_{k+1} \neq 0$ moreover, we have,

$$a_{k+1} = \frac{-\beta_1}{\alpha_{k+1}} b_1 + \cdots + \frac{-\beta_k}{\alpha_{k+1}} b_k + \frac{1}{\alpha_{k+1}} b_{k+1} + \frac{-\alpha_{k+2}}{\alpha_{k+1}} a_{k+1} + \cdots + \frac{-\alpha_n}{\alpha_{k+1}} a_n .$$

Thus, we obtain, $\operatorname{span}(b_1, \cdots, b_k, a_{k+1}, \cdots, a_n) = \operatorname{span}(b_1, \cdots, b_{k+1}, a_{k+2}, \cdots, a_n) = V$.

Next we show $b_1, \cdots, b_{k+1}, a_{k+2}, \cdots, a_n$ are linearly independent.

If for another $\beta_1, \cdots, \beta_{k+1}, \alpha_{k+2}, \cdots, \alpha_n$, $\beta_1 b_1 + \cdots + \beta_{k+1} b_{k+1} + \alpha_{k+2} a_{k+2} + \cdots + \alpha_n a_n = 0$ holds.

Now, since, b_{k+1} has the form (*), and since $a_{k+1} \neq 0$ by induction we have β_{k+1} thus by induction $\beta_1, \cdots, \beta_k, \alpha_{k+1}, \cdots, \alpha_n = 0$. Thus the induction is complete.

Next, we show $n \geq m$. If not $n < m$, then $b_1, \cdots, b_{m-n}, a_1, \cdots, a_n$ are linearly dependent but since $a_1, \cdots, a_n$ is basis, we have $b_1 = \alpha_1 a_1 + \cdots + \alpha_n a_n$ for some $\alpha_1, \cdots, \alpha_n \in \mathbb{F}$. Then we have, $(-1) b_1 + 0 \cdot b_2 + \cdots + 0 \cdot b_{m-n} + \alpha_1 a_1 + \cdots + \alpha_n a_n = 0$. However since $b_1 \neq 0$, a contradiction.

Cor4.

(1) Suppose V has a finite basis with n elements. Any set of linearly independent vectors has $\leq n$ elements. Any spanning set has $\geq n$ elements.

(2) If V has some finite basis then any two bases of V have the same cardinality.

Proof). (1) The first assertion is by last result in thm 3. The second assertion is by Cor2 and the first assertion.

(2) By (1).

Cor5. Building-Up Lemma

If A is a set of linearly independent vectors in the finite dimensional space V then there exists a

basis of V containing A.

Proof). Manifestly by thm 3.

Thm 6. If V is an n-dimensional vector space over F, then $V \simeq F^n$. In particular, any two finite dimensional vector spaces over F of the same dimension are isomorphic.

Proof) Let $v_1, \cdots, v_n$ be a basis of V and let $\varphi : F^n \to V$ be the function which assign the $(a_1, \cdots, a_n)$ the $a_1 v_1 + \cdots + a_n v_n$. Then clearly φ is F-module homomorphism and bijective, so $V \simeq F^n$.

Thm 7 Let V be a vector space over F and let W be a subspace of V. Then V/W is a vector space with $\dim V = \dim W + \dim V/W$.

Proof).

Case 1. $\dim V < \infty$.

Let $v_1, \cdots, v_n$ and $w_1, \cdots, w_m$ be basis of V and W, respectively. Then by Cor 5, there exists extented basis $w_1, \cdots, w_m, v_{m+1}, \cdots, v_n$ of V. Let $\varphi : V \to V/W$ be a natural map which assign the $a_1 w_1 + \cdots + a_m w_m + a_{m+1} v_{m+1} + \cdots + a_n v_n$ the $a_{m+1} v_{m+1} + \cdots + a_n v_n$. We assert that φ is surjective.

For arbitrary $x \in V$, there exists $a_1, \cdots, a_n$ such that $x = a_1 w_1 + \cdots + a_m w_m + a_{m+1} v_{m+1} + \cdots + a_n w_n$. Now, since $a_1 w_1 + \cdots + a_m w_m \in W$, $x + W = (a_{m+1} v_{m+1} + \cdots + a_n w_n) + W$ thus, φ is surjective and hence $\dim V/W = n - m$. Therefore $\dim V = \dim V/W + \dim W$

Case 2. $\dim V = \infty$.

KOKUYO LOOSE-LEAF A-SIZE(ST 6 mm ruled 28 lines

If $\dim W = \infty$, manifestly thus assume that $\dim W < \infty$. Then for infinitely many pair of linearly independent in V, since $\dim W < \infty$, the pair in V/W is also infinitely.

Cor 8. Let $\varphi : V \to U$ be a linear transformation of vector spaces over F. Then $\ker \varphi$ is a subspace of V, $\varphi(V)$ is a subspace of U and $\dim V = \dim \varphi + \dim \varphi(V)$.

Proof) Derived from thm 7.

Cor 9. Let $\varphi : V \to W$ be a linear transformation of vector spaces of the same finite dimension. Then the following are equivalent:

(1) φ is an isomorphism,

(2) φ is injective i.e. $\ker \varphi = 0$,

(3) φ is surjective i.e. $\varphi(V) = W$,

(4) φ sends a basis of V to a basis of W.

Proof).

(1) $\Rightarrow$ (2) obvious.

(2) $\Rightarrow$ (3) by Cor 8

(3) $\Rightarrow$ (4) Since φ is F-module homomorphism

(4) $\Rightarrow$ (1) Since the dimension of V and the dimension of W are the same.

Thm 10 Let V be a vector space over F of dimension n and let W be a vector space over F of dimension m, with bases $\mathcal{B}$, $\mathcal{E}$ respectively. Then the map $\mathrm{Hom}_F(V,W) \to M_{m\times n}(F)$ from the space of linear transformations from V to W to the space of $m\times n$ matrices with coefficients in F defined by $\varphi \mapsto M_{\mathcal{B}}^{\mathcal{E}}(\varphi)$ is a vector space isomorphism. In particular, there is a bijective correspondence between linear transformations and their associated matrix with respect to a fixed choice of bases.

Proof). Let the given function be $\Phi : \mathrm{Hom}(V,W) \to M_{m\times n}(F)$. First we verify Φ is F-module homomorphism. Let $\varphi, \psi \in \mathrm{Hom}(V,W)$ and $a \in F$.

$\Phi(a\varphi+\psi) = (a_{ij})$ with $(a\varphi+\psi)(v_j) = \sum_{1\le i\le m} a_{ij} w_j$

Now, $(a\varphi+\psi)(v_j) = (a\varphi)(v_j) + \psi(v_j)$

$= a(\varphi(v_j)) + \psi(v_j)$

$= a(b_{ij}) + (c_{ij})$ with $\varphi(v_j) = \sum_{1\le i\le m} b_{ij} w_j$, $\psi(v_j) = \sum_{1\le i\le m} c_{ij} w_j$

Thus we obtain $a\sum_{1\le i\le m} b_{ij} w_j + \sum_{1\le i\le m} c_{ij} w_j = \sum_{1\le i\le m} a_{ij} w_j$,

moreover, $\sum_{1\le i\le m} (a\cdot b_{ij} + c_{ij}) w_j = \sum_{1\le i\le m} a_{ij} w_j$. Since $w_1, \cdots, w_m$ are linearly independent we have $a\,b_{ij} + c_{ij} = a_{ij}$ for all i, for all j.

Hence, $(a_{ij}) = (a b_{ij} + c_{ij})$

$= a(b_{ij}) + (c_{ij})$

$= a\,\Phi(\varphi) + \Phi(\psi)$

Therefore, $\Phi(a\varphi+\psi) = a\Phi(\varphi) + \Phi(\psi)$; Φ is an F-module homomorphism.

KOKUYO LOOSE-LEAF A-836GT 6 mm ruled 36 Rule

Now, we show that Φ is bijective. Clearly Φ is injective.

Let $(a_{ij}) \in M_{m\times n}(F')$. We show that there exists a map φ with $\varphi(v_j) = \sum_{1\le i\le m} a_{ij} w_j$ such that it is F'-module homomorphism. However, since $v_1, \dots, v_n$ is basis of V, the F'-module homomorphism determined, thus Φ is surjective.

Cor11 The dimension of $\mathrm{Hom}_{F'}(V, W)$ is $(\dim V)\cdot(\dim W)$.

Proof) By previous theorem, it is enough to show that the dimension of $M_{m\times n}(F')$ is $m\cdot n$.

Clearly, $\{(a_{ij}; a_{kl}=1 \text{ otherwise } 0);\ 1\le k\le m,\ 1\le l\le n\}$ spans $M_{m\times n}(F')$ and since F' is an integral domain, it is linearly independent. (∵ Note that the action is identified with multiplication.)

Thus, $M_{m\times n}(F')$ has a basis with cardinal $m\times n$, so the dimension of $M_{m\times n}(F')$ is mn.

Thm12 With notations as above, $M_{\mathcal{D}}^{\mathcal{E}}(\varphi\circ\psi) = M_{\mathcal{E}}^{\mathcal{E}}(\varphi)\cdot M_{\mathcal{D}}^{\mathcal{B}}(\psi)$, i.e. with respect to a compatible choice of basis, the product of the matrices representing the linear transformations φ and ψ is the matrix representing the composite linear transformation $\varphi\circ\psi$.

Proof) Let $M_{\mathcal{D}}^{\mathcal{E}}(\varphi\circ\psi) = (a_{ij})$ with $(\varphi\circ\psi)(u_j) = \sum_{1\le i\le m} a_{ij} w_i$ for all $1\le j\le k$, $M_{\mathcal{D}}^{\mathcal{B}}(\psi) = (b_{ij})$ with $\psi(u_j) = \sum_{1\le i\le n} b_{ij} v_i$ for all $1\le j\le k$ and, $M_{\mathcal{B}}^{\mathcal{E}}(\varphi) = (c_{ij})$ with $\varphi(v_j) = \sum_{1\le i\le m} c_{ij} w_i$ for all $1\le j\le n$.

Then we have, $(\varphi\circ\psi)(u_j) = \varphi(\psi(u_j))$

$$= \varphi\Big(\sum_{1\le i\le n} b_{ij} v_i\Big)$$

$$= \sum_{1\le i\le n} b_{ij}\,(\varphi(v_i))$$

$$= \sum_{1\le i\le n} b_{ij}\Big(\sum_{1\le l\le m} c_{li} w_l\Big)$$

$$= \sum_{1\le i\le n}\sum_{1\le l\le m} c_{li} b_{ij} w_l$$

$$= \sum_{1\le l\le m}\Big(\sum_{1\le i\le n} c_{li} b_{ij}\Big) w_l$$

Thus, we have $\sum_{1\le i\le m} a_{ij} w_i = \sum_{1\le i\le m}\Big(\sum_{1\le l\le n} c_{il} b_{lj}\Big) w_i$, and since $\{w_1, \cdots, w_m\}$ is a basis, $a_{ij} = \sum_{1\le l\le n} c_{il}\cdot b_{lj}$ for all i and for all j.

This equality show that $(a_{ij}) = (c_{ij})\cdot(b_{ij})$

Thus we have, $M_{\mathcal{B}}^{\mathcal{E}}(\varphi\circ\psi) = M_{\mathcal{B}}^{\mathcal{C}}(\varphi)\cdot M_{\mathcal{B}}^{\mathcal{B}}(\psi)$.

Cor13 Matrix multiplication is associative and distributive (whenever the dimensions are such as to make product defined). An $n\times n$ matrix A is nonsingular iff it is invertible.

Proof) By previous theorem, we easy to show the associativity and distributivity.

Before prove the secound assertion, we verify the following assertion.

Let A be an $n\times n$ matrix and let φ be an F-module homomorphism associated with A. Then A is non-singular iff φ is non-singular.

Let $\mathcal{B} = \{v_1, \cdots, v_n\}$ be a basis of V.

Suppose, A is non-singular. For $\sum_{1\le i\le n} a_i\cdot v_i \in V$ with $\varphi\big(\sum_{1\le i\le n} a_i v_i\big) = 0$, let $\psi : \cdot \mapsto \sum_{1\le i\le n} a_i v_i$ be an F-module homomorphism then we have $(\varphi\circ\psi)(\cdot) = 0$.

And let $x_i = M_{\{i\}}^{\mathcal{B}}(\psi)$ then we have $Ax = M_{\{\cdot\}}^{\mathcal{B}}(\varphi\circ\psi)$ so, $\sum_{1\le i\le n}(Ax)_i v_i = 0$.

Since $\{v_1, \cdots, v_n\}$ are linearly independent, we have $Ax = 0$ then by assumption, $x = 0$ i.e.,

KOKUYO LOOSE-LEAF A-836ST 8 mm ruled 26 lines

$\varphi : \cdot \mapsto 0$ moreover, $\sum_{1 \le i \le n} a_i v_i = 0$ so $\ker \varphi = 0$.

Conversely, suppose φ is non-singular, let x be $n \times 1$ matrix with $Ax = 0$ and let ψ be an F-module homomorphism with $x = M_{\mathcal{E},\mathcal{B}}(\psi)$.

Since $Ax = 0$, $(\varphi \circ \psi)(\cdot) = \sum_{1 \le i \le n} (Ax)_i v_i = 0$, so $\varphi(\psi(\cdot)) = 0$.

Since, φ is non-singular, $\psi(\cdot) = 0$, moreover, $0 = \psi(\cdot) = \sum_{1 \le i \le n} x_i v_i$ and since $\{v_1, \cdots, v_n\}$ are linearly independent, $x_i = 0$ for every i, $x = 0$.

Now, we show the second assertion. Conversely is obvious.

Let V be n-dimensional F-module with basis $\mathcal{B} = \{v_1, \cdots, v_n\}$ and let φ be an F-module homomorphism with $A = M_{\mathcal{B}}(\varphi)$. Now we assert $\mathcal{E} = \{\varphi(v_1), \cdots, \varphi(v_n)\}$ is a bais of V if A is non singular. Since for a_i with $\sum_{1 \le i \le n} a_i \cdot \varphi(v_i) = 0$

$$\sum_{1 \le i \le n} a_i \cdot \varphi(v_i) = 0 \Rightarrow \varphi\left(\sum_{1 \le i \le n} a_i \cdot v_i\right) = 0 \Rightarrow \sum_{1 \le i \le n} a_i \cdot v_i = 0 \Rightarrow a_i = 0 \text{ for all } i.$$

Thus, $\mathcal{E}$ is linearly independent and clearly pairwise distinct, so by Replacement theorem, $\mathcal{E}$ is a basis of V. Thus by Cor 9. φ has the inverse φ^{-1} and let $B := M_{\mathcal{B}}(\varphi^{-1})$ then since we have $\varphi \cdot \varphi^{-1}$ and $\varphi^{-1} \varphi$ are identity, $A \cdot B$ and $B \cdot A$ are identity. A is invertible.

Cor 14

(1) If $\mathcal{B}$ is a basis of the n-dimensional space V. the map $\varphi \mapsto M_{\mathcal{B}}(\varphi)$ is a ring and a vector space isomorphism of $\mathrm{Hom}_F(V, V)$ onto the space $M_n(F)$ of $n \times n$ matrices with coefficient F.

(2) $GL(V) \simeq GL_n(F)$ where $\dim V = n$. In paticular, if F is a finite field the order of the finite group $GL_n(F)$ (which equals to $|GL(V)|$) is given by the formula at the end of Section 1.

Proof). By thm 10, $\varphi \in F\text{-}Mod\ (Hom(V,V), M_n(F))$.

By thm 12, $M_n(F)$ is closed under multiplication and by Cor 13 $M_n(F)$ form the ring.

Let $\Phi : \varphi \mapsto M_{\mathcal{B}}^{\mathcal{B}}(\varphi)$ and $\varphi, \psi \in Hom(V,V)$. Now we have already proved the $\Phi(\varphi+\psi) = \Phi(\varphi) + \Phi(\psi)$ in thm 10 and the $\Phi(\varphi \circ \psi) = \Phi(\varphi) \cdot \Phi(\psi)$.

Therefore, $\Phi \in Rin\ (Hom(V,V), M_n(F))$.

Prop 15. Let F be a subfield of the field K. If W is an m-dimensional vector space over F with basis $w_1, \cdots, w_m$, then $K \otimes_F W$ is an m-dimensional vector space over K with basis $1 \otimes w_1, \cdots, 1 \otimes w_m$.

Proof) By Sec 10.4 Cor 18, we have $K \otimes W \approx W$ with assignment $k \otimes a \mapsto k \cdot a$.

Then the F-module isomorphism assign the $1 \otimes w_i$ the w_i, so $1 \otimes w_1, \cdots, 1 \otimes w_m$ is a basis.

Prop 16. Let V and W be finite dimensional vector spaces over the field F with bases $v_1, \cdots, v_n$ and $w_1, \cdots, w_m$ respectively. Then $V \otimes_F W$ is a vector space over F of dimension mn with basis $v_i \otimes w_j$, $1 \le i \le n$ and $1 \le j \le m$.

Proof) By Sec 10.4 Cor 19, $V \otimes_F W$ is an F-module with basis $v_i \otimes w_j$, $1 \le i \le n$ and $1 \le j \le m$.

Prop 17. Let $\varphi : V \to X$ and $\psi : W \to Y$ be linear transformations of finite dimensional vector spaces. Then the Kronecker product of matrices representing φ and ψ is a matrix representation of $\varphi \otimes \psi$.

Proof). Let $\mathcal{B}_1 = \{v_1, \cdots, v_m\}$ and $\mathcal{E}_1 = \{x_1, \cdots, x_n\}$ be basis of V and X respectively, let $\mathcal{B}_2 = \{w_1, \cdots, w_q\}$ and $\mathcal{E}_2 = \{y_1, \cdots, y_p\}$ be basis of W and Y respectively and let $\mathcal{B} = \{a_{l_1} ; 1 \le l_1 \le mq\}$ with $a_{l_1} = v_{s_1} \otimes w_{s_2}$, $l_1 = (s_1 - 1)q + s_2$ and $\mathcal{E} = \{b_{l_2} ; 1 \le l_2 \le np\}$ with $b_{l_2} = x_{t_1} \otimes y_{t_2}$, $l_2 = (t_1 - 1)p + t_2$

KOKUYO LOOSE-LEAF A-836BT 8 mm ruled 30 lines

respectively.

Then for i, j ($1 \le i \le m$ and $1 \le j \le q$),

$$(\varphi \otimes \psi)(v_i \otimes w_j) = (\varphi(v_i)) \otimes (\psi(w_j))$$

$$= \left(\sum_{1 \le t_1 \le n} M_{\mathcal{E}_1}^{\mathcal{B}_1}(\varphi)_{t_1 i} \cdot x_{t_1} \right) \otimes \left(\sum_{1 \le t_2 \le p} M_{\mathcal{E}_2}^{\mathcal{B}_2}(\psi)_{t_2 j} \, y_{t_2} \right)$$

$$= \sum_{1 \le t_1 \le n} \sum_{1 \le t_2 \le p} M_{\mathcal{E}_1}^{\mathcal{B}_1}(\varphi)_{t_1 i} \cdot M_{\mathcal{E}_2}^{\mathcal{B}_2}(\psi)_{t_2 j} \, (x_{t_1} \otimes y_{t_2})$$

$$= \sum_{\substack{1 \le l_2 \le np \\ l_2 = (t_1 - 1)p + t_2}} M_{\mathcal{E}_1}^{\mathcal{B}_1}(\varphi)_{t_1 i} \cdot M_{\mathcal{E}_2}^{\mathcal{B}_2}(\psi)_{t_2 j} \, b_{l_2}$$

and we have

$$(\varphi \otimes \psi)(v_i \otimes w_j) = (\varphi \otimes \psi)(a_{(i-1)q + j})$$

$$= \sum_{1 \le l_2 \le np} M_{\mathcal{E}}^{\mathcal{B}}(\varphi \otimes \psi)_{l_2 (i-1)q + j} \, b_{l_2}.$$

Since $b_1, \cdots, b_{np}$ are linearly independent, $M_{\mathcal{E}_1}^{\mathcal{B}_1}(\varphi)_{t_1 i} \cdot M_{\mathcal{E}_2}^{\mathcal{B}_2}(\psi)_{t_2 j} = M_{\mathcal{E}}^{\mathcal{B}}(\varphi \otimes \psi)_{l_2 l_1}$ with $l_1 = (i-1)q + j$ and $l_2 = (t_1 - 1)p + t_2$. Hence, $M_{\mathcal{E}_1}^{\mathcal{B}_1}(\varphi) \otimes M_{\mathcal{E}_2}^{\mathcal{B}_2}(\psi) = M_{\mathcal{E}}^{\mathcal{B}}(\varphi \otimes \psi)$.

Prop 18. With notation as above, $\{v_1^*, \cdots, v_n^*\}$ is a basis of V^*. In particular, if V is finite dimensional then V^* has the same dimension as V.

Proof) By Cor 11 we have $\dim V^* = \dim \mathrm{Hom}(V, F) = \dim V \times \dim F = n$.

Let $a_i \in F$ with $\sum_{1 \le i \le n} a_i \, v_i^* = 0$ this show for every i, $a_i \cdot v_i^*(v_i) = 0$ so, $a_i = 0$.

So, $v_1^*, \cdots, v_n^*$ are linearly independent then by Replacement theorem, $v_1^*, \cdots, v_n^*$ is a basis of V^*.

Thm 19. There is a natural injective linear transformation from V to V^{**}. If V is finite dimensional then this linear transformation is an isomorphism.

Proof) For $v \in V$ define $E_v : V^* \to F$; $f \mapsto f(v)$ then we have $E_v \in V^{**}$. Let $\varphi : V \to V^{**}$; $v \mapsto E_v$.

For $v, w \in V$ and $\alpha \in F$,

$$\varphi(v + \alpha w)(f) = f(v + \alpha w) = f(v) + \alpha \cdot f(w) = (\varphi(v) + \alpha \cdot \varphi(w))(f).$$

Thus, φ is an F-module homomorphism. Now we assert φ is injective.

Let v be nonzero elements in V then there exists a basis $\mathcal{B}$ of V containing v and let f be an F-module homomorphism which assign $v \mapsto 1$, $w \mapsto 0$ for all $w \in \mathcal{B} \setminus \{v\}$. Then $f \in V^*$ and $E_v(f) = 1$ thus $\varphi(v) = E_v$ is not zero in V^{**}. This assert $\ker \varphi = 0$ i.e. φ is injective.

Since the dimension of V is finite, by prop18, V^* has the same dimension, so is V^{**}. And by cor 9, we obtain the natural map is an isomorphism.

Thm20. With notations as above, φ^* is a linear transformation from W^* to V^* and $M_{\mathcal{E}^*}^{\mathcal{B}^*}(\varphi^*)$ is the transpose of the matrix $M_{\mathcal{B}}^{\mathcal{E}}(\varphi)$.

Proof) Let $\mathcal{E} = \{v_1, \cdots, v_n\}$ and $\mathcal{B} = \{w_1, \cdots, w_m\}$ and let $M_{\mathcal{E}^*}^{\mathcal{B}^*}(\varphi^*) = (a_{ij})$ with $\varphi^*(w_j^*) = \sum_{1 \le i \le n} a_{ij} v_i$ for all $1 \le j \le m$.

For $1 \le k \le n$,

$$\left(\sum_{1 \le i \le n} a_{ij} v_i^*\right)(v_k) = \sum_{1 \le i \le n} a_{ij} v_i^*(v_k)$$

$$= a_{kj}.$$

KOKUYO LOOSE-LEAF A-836BT 8 mm ruled x30 lines

$$\varphi^*(w_j^*)(v_k) = w_j^*(\varphi(v_k))$$

$$= w_j^*\left(\sum_{1\le l\le m} a_{lk}\cdot w_l\right)$$

$$= b_{jk}$$

where $M_{\mathcal{B}}^{\mathcal{E}}(\varphi) = (b_{ij})$.

Then we have $a_{kj} = b_{jk}$ for $1\le k\le m$ and for $1\le j\le m$.

Therefore, $M_{\mathcal{E}^*}^{\mathcal{B}^*}(\varphi^*)$ is the transpose of the matrix $M_{\mathcal{B}}^{\mathcal{E}}(\varphi)$.

Cor 21. For any matrix A, the row rank of A equals the column of rank of A.

Before prove the given assertion, we verify two propositions.

First, we show the followings.

Let $\varphi\in \mathrm{Hom}(F^n, F^m)$ and let $\mathcal{B}$ be a basis of F^n, $\mathcal{E}$ be a natural basis of F^m. Then the set of columns of $M_{\mathcal{E}}^{\mathcal{B}}(\varphi)$ spans $\mathrm{im}\,\varphi$ and the rank of φ is equals to the column rank of $M_{\mathcal{E}}^{\mathcal{B}}(\varphi)$.

For every v_i we have $\varphi(v_i) = \sum_{1\le j\le m} M_{\mathcal{E}}^{\mathcal{B}}(\varphi)_{ji}\, v_j = (M_{\mathcal{E}}^{\mathcal{B}}(\varphi)_{1i}, \cdots, M_{\mathcal{E}}^{\mathcal{B}}(\varphi)_{mi})$ and since $\{v_i\}$ is a basis, $\mathrm{span}\{\varphi(v_i)\} = \mathrm{im}\,\varphi$ since φ is F-module homomorphism.

Therefore, the set of columns of $M_{\mathcal{E}}^{\mathcal{B}}(\varphi)$ spans $\mathrm{im}\,\varphi$.

The secound assertion derived from thm 6.

Secound, we verify the followings,

Let V be finite dimensional and W^* be a submodule of V^* then, $\dim V = \dim(W^*) + \dim \mathrm{Ann}(W^*)$.

If $\dim V^* = \dim W^*$ clearly holds. Let $\mathcal{E}^* = \{w_1^*, \cdots, w_m^*\}$ be a basis of W^* and let $\mathcal{B}^* = \{w_1^*, \cdots, w_m^*, v_{m+1}^*, \cdots, v_{m+n}^*\}$ be a basis of V^*. Where $\mathrm{Ann}(W^*) = \{r \in V ; f(r) = 0 \text{ for all } f \in W^*\}$

Now we assert $\{v_{m+i} ; 1 \le i \le n\}$ spans $\mathrm{Ann}(W^*)$.

First we assert $v_{m+i} \in \mathrm{Ann}(W^*)$ for every i.

For every $\sum_{1 \le j \le m} a_j w_j^* \in W^*$,

$$\left(\sum_{1 \le j \le m} a_j \cdot w_j^*\right)(v_{m+i}) = \sum_{1 \le j \le m} a_j \cdot w_j^*(v_{m+i})$$

$$= \sum_{1 \le j \le m} a_j \cdot 0$$

$$= 0$$

Thus, $\mathrm{span}\{v_{m+i} ; 1 \le i \le n\} \subseteq \mathrm{Ann}(W^*)$.

And for, $\sum_{1 \le i \le m} a_i \cdot w_i + \sum_{1 \le i \le n} a_{m+i} \cdot v_{m+i} \in \mathrm{Ann}(W^*)$.

For every w_l^*, $1 \le l \le m$, we have $w_l^*\left(\sum_{1 \le i \le m} a_i \cdot w_i + \sum_{1 \le i \le n} a_{m+i} v_{m+i}\right) = 0$ thus $a_l = 0$ for every l. Therefore, $\mathrm{Ann}(W^*) = \mathrm{span}\{v_{m+i} ; 1 \le i \le n\}$ and since every v_{m+i} are linearly idependent so, $\dim \mathrm{Ann}(W^*) = n$.

Hence, $\dim V = \dim(W^*) + \dim \mathrm{Ann}(W^*)$. ····· (1)

KOKUYO LOOSE-LEAF A-868DT 6 mm ruled 30 lines

Now we show the Cor 21.

Let φ be an F-module homomorphism from V to W. By (*) and thm 20 it is enough to show that the rank of φ and the rank of φ^* are the same.

Since $f \in \ker(\varphi^*) \iff \varphi^*(f) = 0$

$\iff f \circ \varphi(v) = 0$ for all $v \in V$.

$\iff f(x) = 0$ for all $x \in \varphi(V)$

$\iff f \in \mathrm{Ann}(\varphi(V))$

Hence, we have $\ker(\varphi^*) = \mathrm{Ann}(\varphi(V))$ ... (2) and by Cor 8 we have $\dim W^* = \dim \ker \varphi^* + \dim \varphi^*(W^*)$ ... (3).

Thus, $\dim(\varphi^*(W^*)) = \dim W^* - \dim \ker \varphi^*$ (by 3)

$= \dim W - \dim \mathrm{Ann}(\varphi(V))$ (by (2))

$= \dim(\varphi(V))$ (by 1).

Prop 22. Let φ be an n-multilinear alternating function on V. Then

(1) $\varphi(v_1, \cdots, v_{i-1}, v_{i+1}, v_i, v_{i+2}, \cdots, v_n) = -\varphi(v_1, v_2, \cdots, v_n)$ for any $i \in \{1, \cdots, n-1\}$, i.e., the value of φ on an n-tuple is negated if two adjacent components are interchanged.

(2) For each $\sigma \in S_n$, $\varphi(v_{\sigma(1)}, \cdots, v_{\sigma(n)}) = \varepsilon(\sigma)\varphi(v_1, \cdots, v_n)$, where $\varepsilon(\sigma)$ is the sign of the permutation σ.

(3) If $v_i = v_j$ for any pair of distinct $i, j \in \{1, 2, \cdots, n\}$ then $\varphi(v_1, \cdots, v_n) = 0$.

(4) If v_i is replaced by $v_i + \alpha v_j$ in $(v_1, \cdots, v_n)$ for any $j \neq i$ and any $\alpha \in R$, the value of φ on this n-tuple is not changed.

Proof).

(1) Let $1 \leq i \leq n-1$ and fix v_j for $1 \leq j \leq i-1$, $i+2 \leq j \leq n$ and define the function ψ as $\psi(x, y) := \varphi(v_1, \cdots, v_{i-1}, x, y, v_{i+1}, \cdots, v_n)$ then it is enough to show that $\psi(x, y) = -\psi(x, y)$.

Since φ is alternating, $0 = \psi(x+y, x+y) = \psi(x, x) + \psi(x, y) + \psi(y, x) + \psi(y, y) = \psi(x, y) + \psi(y, x)$.

Thus we have, $\psi(x, y) = -\psi(y, x)$.

(2) Let $\sigma = \tau_1 \cdots \tau_k$ with $\tau_i = (j, j+1)$ for some j.

Then, we have $\varepsilon(\tau_i) = -1$ for every i and $\varepsilon(\sigma) = \varepsilon(\tau_1) \cdots \varepsilon(\tau_k)$, we have $\varphi(v_{\sigma(1)}, \cdots, v_{\sigma(n)}) = \varepsilon(\sigma)\, \varphi(v_1, \cdots, v_n)$.

(3) For $(i+1, j) \in S_n$ by (2) we have, $\varphi(v_1, \cdots, v_n) = \varepsilon((i+1, j))^{-1} \cdot \varphi(v_1, \cdots, v_i, v_j, \cdots)$ so, $\varphi(v_1, \cdots, v_n) = 0$.

(4) $\varphi(v_1, \cdots, v_{i-1}, \alpha \cdot 0, v_{i+1}, \cdots, v_{j-1}, v_j, v_{j+1}, \cdots, v_n)$

$= \varphi(v_1, \cdots, v_{i-1}, \alpha v_j, v_{i+1}, \cdots, v_{j-1}, 0, v_{j+1}, \cdots, v_n)$

we obtain, $\varphi(v_1, \cdots, v_{i-1}, \alpha v_j, v_{i+1}, \cdots, v_{j-1}, v_j, v_{j+1}, \cdots, v_n) = 0$ thus, φ is not change whenever replacing v_i by $v_i + \alpha v_j$ with $i \neq j$.

KOKUYO LOOSE-LEAF J-80EDT 6 mm ruled x 30 lines

Prop 23. Assume φ is an n-multilinear alternating function on V and that for some $v_1, \cdots, v_n$ and $w_1, \cdots, w_n \in V$ and some $a_{ij} \in R$ we have $w_1 = a_{11}v_1 + \cdots + a_{n1}v_n, \cdots, w_n = a_{1n}v_1 + \cdots + a_{nn}v_n$. Then $\varphi(w_1, \cdots, w_n) = \sum_{\sigma \in S_n} \varepsilon(\sigma)\, a_{\sigma(1)1} \cdots a_{\sigma(n)n}\, \varphi(v_1, \cdots, v_n)$.

Proof) Let $N = \{1, \cdots, n\}$.

$$\varphi(w_1, \cdots, w_n) = \sum_{f \in N^N} \varphi(a_{f(1)1}v_{f(1)}, \cdots, a_{f(n)n}v_{f(n)})$$

$$= \sum_{\substack{f \in N^N \\ f \text{ is injective}}} a_{f(1)1} \cdots a_{f(n)n}\, \varphi(v_{f(1)}, \cdots, v_{f(n)}) + \sum_{\substack{f \in N^N \\ f \text{ is not injective}}} a_{f(1)1} \cdots a_{f(n)n}\, \varphi(v_{f(1)}, \cdots)$$

Now, if f is not injective, for some distinct i and j, $v_{f(i)} = v_{f(j)}$ holds. Then by (3) of prop 22, we have $\varphi(v_{f(1)}, \cdots, v_{f(n)}) = 0$.

Since, N is finite, f is surjective whenever f is injective. Then by (2) of prop 22, we have $\varphi(v_{f(1)}, \cdots, v_{f(n)}) = \varepsilon(f)\, \varphi(v_1, \cdots, v_n)$ for injection f.

Therefore, we obtain $\varphi(w_1, \cdots, w_n) = \sum_{\sigma \in S_n} \varepsilon(\sigma)\, a_{\sigma(1)1} \cdots a_{\sigma(n)n}\, \varphi(v_1, \cdots, v_n)$.

Thm 24. There is a unique $n \times n$ determinant function on R and it can be computed for any $n \times n$ matrix (a_{ij}) by the formula: $\det(a_{ij}) = \sum_{\sigma \in S_n} \varepsilon(\sigma)\, a_{\sigma(1)1} \cdots a_{\sigma(n)n}$.

Proof) First we assert det is an alternating function.

Let i with $M(\varphi)_{ki} = M(\varphi)_{k\,i+1}$ for every $1 \le k \le n$ and for $\sigma \in S_n$, define a formula P as $P(\sigma) \Leftrightarrow \sigma(i) < \sigma(i+1)$ and let $\tau : N \to N$, $i \mapsto i+1$, $i+1 \mapsto i$, $j \mapsto j$.

$$\det(a_{ij}) = \sum_{\sigma \in S_n} \varepsilon(\sigma)\, M(\varphi)_{\sigma(1)1} \cdots M(\varphi)_{\sigma(n)n}$$

$$= \sum_{\substack{\sigma \in S_n \\ P(\sigma)}} \Big((\varepsilon(\sigma)\, M(\varphi)_{\sigma(1)1} \cdots M(\varphi)_{\sigma(n)n}) + (\varepsilon(\sigma\tau)\, M(\varphi)_{(\sigma\tau)(1)1} \cdots M(\varphi)_{(\sigma\tau)(n)n}) \Big)$$

$$= \sum_{\substack{\sigma \in S_n \\ P(\sigma)}} \left(\left(\varepsilon(\sigma) M(\varphi)_{\sigma(1)1} \cdots M(\varphi)_{\sigma(n)n} \right) + \left(-\varepsilon(\sigma) M(\varphi)_{\sigma(1)1} \cdots M(\varphi)_{\sigma(i+1)i} M(\varphi)_{\sigma(i)i+1} \cdots \right) \right)$$

$$= \sum_{\substack{\sigma \in S_n \\ P(\sigma)}} 0$$

$$= 0$$

Thus, Axiom (1) holds.

If φ is an identity i.e. $\varphi(v_i) = w_i$. Where $\{v_1, \cdots, v_n\}$ and $\{w_1, \cdots, w_n\}$ are basis of V and W with $\varphi \in \mathrm{Hom}(V, W)$. Then, $\sum_{1 \le i \le n} a_{ij} \cdot w_i = w_i$ so since $w_1, \cdots, w_n$ are linearly independent, $a_{ii} = 1$ and $a_{ji} = 0$ if $i \neq j$ for every i.

Therefore, $\det(I) = \sum_{\sigma \in S_n} \varepsilon(\sigma)\, a_{\sigma(1)1} \cdots a_{\sigma(n)n}$

$$= \sum_{\substack{\sigma \in S_n \\ \sigma \neq id}} \varepsilon(\sigma)\, a_{\sigma(1)1} \cdots a_{\sigma(n)n} + \sum_{\substack{\sigma \in S_n \\ \sigma = id}} \varepsilon(\sigma)\, a_{\sigma(1)1} \cdots a_{\sigma(n)n}$$

$$= \varepsilon(id)$$

$$= 1$$

Thus, Axiom (2) holds.

Next, we verify the uniqueness. Suppose Ψ be a function satisfies axiom (1) and (2). Then since Ψ is an alternating function,

$$\Psi(\varphi(v_1), \cdots, \varphi(v_n)) = \sum_{\sigma \in S_n} \varepsilon(\sigma)\, a_{\sigma(1)1} \cdots a_{\sigma(n)n}\, \varphi(w_1, \cdots, w_n)$$

where $(a_{ij}) := M(\varphi)_{ij}$ and by axiom (2), $\varphi(w_1, \cdots, w_n) = 1$.

Thus, φ is the function det.

Cor 25. The determine is an n-multilinear function of the rows of $M_{n \times n}(R)$ and for any $n \times n$

KOKUYO LOOSE-LEAF A-836BT 6 mm ruled x 35 lines

matrix A, $\det A = \det(A^t)$, where A^t is the transpose of A.

Proof.)

$$\det(A^t) = \sum_{\sigma \in S_n} \varepsilon(\sigma)\, a_{1\sigma(1)} \cdots a_{n\sigma(n)}$$

$$= \sum_{\sigma \in S_n} \varepsilon(\sigma^{-1})\, a_{1\sigma^{-1}(1)} \cdots a_{n\sigma^{-1}(n)}$$

$$= \sum_{\sigma \in S_n} \varepsilon(\sigma)\, a_{\sigma(\sigma^{-1}(1))\sigma^{-1}(1)} \cdots a_{\sigma(\sigma^{-1}(n))\sigma^{-1}(n)}$$

$$= \det A$$

Thm26 Cramer's Rule

If $A_1, \cdots, A_n$ are the columns of an $n \times n$ matrix A and $B = \beta_1 A_1 + \cdots + \beta_n A_n$, for some $\beta_1, \cdots, \beta_n \in R$, then $\beta_i \det A = \det(A_1, \cdots, A_{i-1}, B, A_{i+1}, \cdots, A_n)$.

Proof) Directly derived from (3) of prop23.

Cor27 If R is an integral domain, then $\det A = 0$ for $A \in M_n(R)$ iff the columns of A are R-linearly dependent as elements of the free R-module of rank n. Also, $\det A = 0$ iff the rows of A are R-linearly dependent.

Proof) Since $\det A = \det A^t$ the first assertion implies the secound.

First, assume that column of A^n are linearly independent and $0 = \beta_1 A_1 + \cdots + \beta_n A_n$ is a dependence relation on the columns of A with $\beta_i \neq 0$. Then by Cramer's Rule we have $\beta_i \det A = 0$ since R is an integral domain. $\det A = 0$.

Conversely, assume that the columns of are linearly independent. Let F be the quotient field associated by R then every R-module endomorphism on R^n may be considered as an F-module endo-

morphism on F^n. Now every F-linear combination of the columns of A gives an R-linear combination by multiplying every denominator of coefficient. Hence, colums of A, $A_1, \cdots, A_n$, are linearly independent so is a basis of F^n.

Let $\varphi : F^n \to F^n ; A_i \mapsto A_i$ be an identity F-module homomorphism. If $\det(A_1, \cdots, A_n) = 0$, by prop 23 $\det(\varphi) = 0$. However $\det(\varphi) = 1$. This contradicts $1 \neq 0$.

Thm 28. For matrices $A, B \in M_{n\times n}(R)$, $\det(AB) = \det(A)\cdot\det(B)$.

Proof) Let φ and ψ be R-module homomorphism with $M_{\mathcal{E}}^{\mathcal{B}}(\varphi) = B$ and $M_{\mathcal{B}}^{\mathcal{E}}(\psi) = A$. where $\mathcal{B} = \{v_1, \cdots, v_n\}$, $\mathcal{E} = \{w_1, \cdots, w_n\}$ are basis.

Now, $(A\cdot B)_j = (\psi\circ\varphi)(v_j)$

$$= \psi\left(\sum_{1\le k\le n} B_{kj}\cdot w_k\right)$$

$$= \sum_{1\le k\le n} B_{kj}\cdot \psi(w_k)$$

$$= \sum_{1\le k\le n} B_{kj}\cdot A_k$$

Therefore by prop 23,

$$\det(A\cdot B) = \sum_{\sigma\in S_n} \varepsilon(\sigma)\cdot B_{\sigma(1)1}\cdots B_{\sigma(n)n}\cdot \det(A)$$

$$= \det B\cdot \det A.$$

Thm 29 (The cofactor Expansion Formula along the ith rows)

If $A = (a_{ij})$ is an $n\times n$ matrix, then for each fixed $i \in \{1, 2, \cdots, n\}$ the determinant of A can be computed from the formula $\det A = (-1)^{i+1} a_{i1}\det A_{i1} + \cdots + (-1)^{i+2} a_{in}\det A_{in}$.

KOKUYO LOOSE-LEAF

Proof). For an $n \times n$ matrix A and i, $1 \le i \le n$, define $D_n(A) = \sum_{1 \le j \le n} (-1)^{i+j} a_{ij} \det A_{ij}$.

We verify D_n is the determinant function by induction on n.

If $n = 2$. Let $\mathcal{B} = \{v_1, v_2\}$ be a basis of 2-dimensional R-module and let φ be an R-module homomorphism and let $a_{11}, a_{21}, a_{12}, a_{22}$ in R with $\varphi(v_1) = a_{11}v_1 + a_{21}v_2$ and $\varphi(v_2) = a_{12}v_1 + a_{22}v_2$. Then we have $D_n(\varphi) = (-1)^{i+1} a_{i1} \cdot \det A_{i1} + (-1)^{i+2} a_{i2} \cdot \det A_{i2}$.

If $i = 1$, $D_2(\varphi) = a_{11}a_{22} - a_{12} \cdot a_{21}$,

If $i = 2$ $D_2(\varphi) = -a_{21} \cdot a_{12} + a_{22}a_{11}$

Thus, $D_2(\varphi) = a_{11}a_{22} - a_{12} \cdot a_{21}$.

On the other hand, $\det(\varphi) = \varepsilon(id)\, a_{11}a_{22} + \varepsilon(12) \cdot a_{21}a_{12} = a_{11}a_{22} - a_{12}a_{21}$.

Assume $n \ge 3$. We check D_n satisfies axiom (1) and (2).

(Axiom 1) First, we verify D_n is multilinear, D_n is linearly in the k-coordinate for every k.

Since every A_{ij} is multilinear, and A_{ik} does not depend on k-column of A. Thus, D_n is multilinear. Next, we verify D_n is alternative, assume k-column and $k+1$ column are the same. Then by assumption, for $j \neq k, k+1$, $\det A_{ij} = 0$. Since $A_{ik} = A_{ik+1}$ and $a_{ik} = a_{ik+1}$, $a_{ik} \cdot \det(A_{ik}) = a_{ik+1} \det(A_{ik+1})$ moreover, $(-1)^{i+k} a_{ik} \det A_{ik} + (-1)^{i+k+1} a_{ik+1} \det A_{ik+1} = 0$

Thus, $D_n(A) = 0$, D_n is altenative.

Therefore D_n satisfy Axiom (1).

(Axiom 2) Since, if $i \neq j$, $\det(A_{ij}) = 0$, clearly $D_n(A) = 1$.

Thm 30 (Cofactor Formula for the Inverse of a Matrix).

Let $A = (a_{ij})$ be an $n \times n$ matrix and let B be the transpose of its matrix of cofactors, i.e., $B = (\beta_{ij})$, where $\beta_{ij} = (-1)^{i+j} \det A_{ji}$, $1 \le i, j \le n$. Then $AB = BA = (\det A) \cdot I$. Moreover, $\det A$ is a unit in R iff A is a unit in $M_{n \times n}(R)$; in this case the matrix $\frac{1}{\det A} B$ is the inverse of A.

Proof). Let $\mathcal{B} = \{v_1, \cdots, v_n\}$ be a basis of n-dimensional R-module and let φ and ψ be R-module homomorphisms which representation are A and B respectively. Let i, $1 \le i \le n$.

$$(\psi \circ \varphi)(v_i) = \sum_{1 \le j \le n} \Big(a_{ji} \sum_{1 \le k \le n} (-1)^{k+j} \det A_{jk} \cdot v_k \Big)$$

$$= \sum_{1 \le j \le n} a_{ji} (-1)^{i+j} \det A_{ji} \cdot v_i + \sum_{\substack{1 \le k \le n \\ k \ne i}} \Big(\Big(\sum_{1 \le j \le n} a_{ji} (-1)^{k+j} \det A_{jk} \Big) v_k \Big)$$

Now, let $\bar{\varphi}(v_k) = \begin{cases} \varphi(v_k) & \text{if } k \ne i \\ \varphi(v_i) & \text{if } k = i. \end{cases}$ and let $\bar{A} := M(\bar{\varphi})$ then clearly we have

$\det(\bar{\varphi}) = 0$.

$$\sum_{1 \le j \le n} a_{ji} (-1)^{k+j} \det A_{jk} = \sum_{1 \le j \le n} (-1)^{k+j} \bar{a}_{jk} \det \bar{A}_{jk} = \det \bar{A} = 0.$$

Therefore, $(\psi \circ \varphi)(v_i) = \det A \cdot v_i + 0 = \det A \cdot v_i$. Hence $\psi \circ \varphi = \det A \cdot id$.

And similarly, we have $\varphi \circ \psi = \det A \cdot id$.

The secound assention is by thm 30 and first assention.

Thm 31 If M is any R-module over the commutative ring R then

(1) $T(M)$ is an R-algebra containing M with multiplication defined by mapping

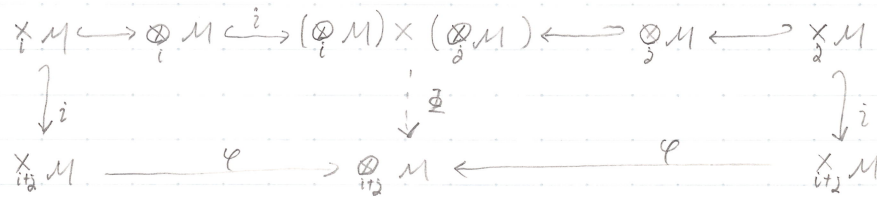
$$(m_1 \otimes \cdots \otimes m_i)(m'_1 \otimes \cdots \otimes m'_j) = m_1 \otimes \cdots \otimes m_i \otimes m'_1 \otimes \cdots \otimes m'_j$$

KOKUYO CAMPUS-LEAF A-836B1 6 mm ruled / 36 lines

and extended to sums via the distributive laws. With respect to this multiplication $T^i(M)\,T^j(M) \subseteq T^{i+j}(M)$.

(2) Universal Property. If A is any R-algebra and $\varphi: M \to A$ is an R-module homomorphism, then there is a unique R-algebra homomorphism $\Phi: T(M) \to A$ such that $\Phi|_M = \varphi$.

Proof) (1) Since, $\varphi : \underset{i\geq 1}{\times} M \to \underset{i\geq 1}{\otimes} M$ is multilinear, there exists unique $\tilde{\varphi}$ as $T\tilde{F}\Theta C$:



with disired assignment. Thus the disired multiplication is well-defined.

Since, M is embedded to $T(M)$, clearly $T(M)$ is an R-algebra.

(2) Since, $\psi : \underset{k}{\times} M \to A\,;\,(m_1, \cdots, m_k) \mapsto \varphi(m_1) \cdots \varphi(m_k)$ is a multilinear and induce the module homomorphism $\Phi_k : T^k(M) \to A$. We have $\Phi : T(M) \to A$ with $\Phi|_M = \varphi$.

Prop 32. Let V be a finite dimensional vector space over the field F with basis $\mathcal{B} = \{v_1, \cdots, v_n\}$. Then the k-tensors $v_{i_1} \otimes \cdots \otimes v_{i_k}$ with $v_{i_j} \in \mathcal{B}$ are a vector space basis of $T^k(V)$ over F. In particular, $\dim_F(T^k(V)) = n^k$.

Proof) This follows immediately from prop. 11.2.16.

Prop 33. Let S be a graded ring, let I be a graded ideal in S and let $I_k = I \cap S_k$ for all $k \geq 0$. Then S/I is naturally a graded ring whose homogeneous component of degree k is isomorphic to S_k/I_k

Proof). Let $\varphi : S \longrightarrow \oplus (S_i/I_i)$; $s_i \longmapsto s_i + I_i$ factorwise.

First we assert $\ker \varphi = I$.

(c) $\forall a \in S$ with $\varphi(a) = 0$ and let $a = (a_1, \cdots, a_i, \cdots)$ then by assignment of φ, $a_i + I_i = 0$ $a_i \in I_i$ for every i. Thus, $a \in \oplus I_i = I$.

(⊃) $\forall i \in I \subset S$ and let $i = (i_1, \cdots, i_j, \cdots)$. By assignment of φ and $i_j \in I_j$ for every j, we have $\varphi(i) = 0$.

Next, we show S/I is graded ring. It suffice to show that $(a+I_i)(b+I_j) = ab + I_{i+j}$ for $a \in S_i$ and $b \in S_j$ is well-defined.

For $x \in I_i$ and $y \in I_j$.

$$(a+x+I_i)(b+y+I_j) = (a+x)(b+y) + I_{i+j}$$

$$= ab + ay + xb + xy + I_{i+j}.$$

Now, by $x \in I_i \subset S_i$ and $y \in I_j \subset S_j$, $xb, ya \in S_{i+j}$ moreover, since $xb, ya \in I$, $xb, ya \in I_{i+j}$. and clearly $xy \in I_{i+j}$. Therefore, $(a+x+I_i)(b+y+I_j) = ab + I_{i+j}$

Thm 34 Let M be an R-module over the commutative R and let $S(M)$ be its symmetric algebra.

(1) The kth symmetric power, $S^k(M)$, of M is equal to $M \otimes \cdots \otimes M$ (k-factors) modulo the submodule generated by all elements of the form

$$(m_1 \otimes \cdots \otimes m_k) - (m_{\sigma(1)} \otimes \cdots \otimes m_{\sigma(k)})$$

for all $m_i \in M$ and all permutations σ in the symmetric group S_k.

KOKUYO LOOSE-LEAF A-836BT 6mm ruled 36 lines

(2) Universal Property for Symmetric Multilinear Maps

If $\varphi : M \times \cdots \times M \to N$ is a symmetric k-multilinear map over R then there is a unique R-module homomorphism $\bar{\varphi} : S^k(M) \to N$ such that $\varphi = \bar{\varphi} \circ \tau$, where $\tau : M \times \cdots \times M \to S^k(M)$ is the map defined by $\tau(m_1, \cdots, m_k) = m_1 \otimes \cdots \otimes m_n \bmod C(M)$.

(3) Universal Property for maps to commutative R-algebras

If A is any commutative R-algebra and $\varphi : M \to A$ is an R-module homomorphism, then there is a unique R-algebra homomorphism $\bar{\varphi} : S(M) \to A$ such that $\bar{\varphi}|_M = \varphi$.

Proof)

(1) It is enough to show that $C^k(M) = C^k = \{(m_1 \otimes \cdots \otimes m_k) - (m_{\sigma(1)} \otimes \cdots \otimes m_{\sigma(k)}) \cdots (*_\sigma)\}$.

Note that since $C^k(M)$ is an ideal generated by homogeneous elements, every element has a form

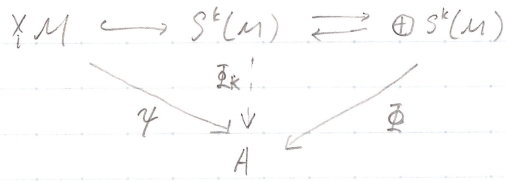
$$m_1 \otimes \cdots \otimes m_{i-1} \otimes (m_i \otimes m_{i-1} - m_{i-1} \otimes m_i) \otimes \cdots \otimes m_k \cdots\cdots (*_i)$$

Since, $(*_i) = (*_{(i\ i+1)})$, $C^k(M) \subset C^k$. For every $\sigma \in S_k$ there exists $\tau \in S_k$ and i such that $\sigma = (i\ i+1)\tau$. Then by renaming subscript by τ, we have $(*_\sigma) = (*_i)$, $C^k \subset C^k(M)$.

(2) This show by the following diagram and note that since φ is symmetric, $\varphi' \circ \tau = 0$.

$$\begin{array}{ccccc} \overset{k}{\times} M & \hookrightarrow & T^k(M) & \overset{\tau}{\leftrightarrows} & C^k(M) \\ {\scriptstyle\varphi}\downarrow & \swarrow{\scriptstyle\varphi'} & & & \downarrow{\scriptstyle \text{cokern}\,\tau} \\ N & \overset{\bar{\varphi}}{\leftarrow} & S^k(M) & & \end{array}$$

(3) Since, $\varphi : \overset{k}{\times} M \to A\ ;\ (m_1, \cdots, m_k) \mapsto \varphi(m_1) \cdots \varphi(m_k)$ is a multilinear map, we have the following;



Cor35. Let V be an n-dimensional vector space over the field F. Then $S(V)$ is isomorphic as a graded F-algebra to the ring of polynomials in n variables over F. In particular, $\dim_F(S^k(V)) = \binom{k+n-1}{n-1}$.

Proof). Let $\mathcal{B} = \{v_1, \cdots, v_n\}$ be a basis then by prop 32. there exists one to one correspondance from $\mathcal{B})^k$ to a basis $\mathcal{E}^k$ of $T^k(V)$.

Now, we define a relation $b \sim b'$ in $(\mathcal{B}^k)$ $\nexists$ $b_i = b'_{\sigma(i)}$ for $1 \le i \le k$ for some $\sigma \in S_k$. Manifestly, $\sim$ is an equivalent class. Since, by thm 34 (1), we have $S^k(V) = T^k(V)/\sim$, we obtain $\mathcal{E}^k/\sim$ is a basis of $S^k(V)$.

We repicking every representative A_i for equivalent class $\mathcal{E}^k/\sim$ as $\underbrace{v_1 \otimes \cdots \otimes v_1}_{a_i^1 \text{ factors}} \otimes v_2 \otimes \cdots \otimes \underbrace{v_n \otimes \cdots \otimes v_n}_{a_i^n \text{ factors}}$, written $(v_1^{a_i^1}, \cdots, v_n^{a_i^n})$ with $\sum_{1 \le j \le n} a_j^i = k$ for every i. Moreover, every representative corresponding to monic monomials of degree k in $F[x_1, \cdots, x_n]$.

Thus, $S^k(V)$ over F isomorphic to $F[x_1, \cdots, x_n]$.

Finally, we verify "in paticular". The dimension of $S^k(V)$ is the number of pair $a_1, \cdots, a_n \in \mathbb{N}$ such that $\sum_{1 \le j \le n} a_j = k$. Thus, $\dim(S^k(V)) = \binom{k+n-1}{n-1}$.

Thm36 Let M be an R-module over the commutative ring R and let $\Lambda(M)$ be its exterior algebra.

(1) The kth exterior power, $\Lambda^k(M)$, is equal to $M \otimes \cdots \otimes M$ (k factors) modulo the submodule generated by all elements of the form

$m_1 \otimes m_2 \otimes \cdots \otimes m_k$ where $m_i = m_j$ for some $i \neq j$.

In paticular, $m_1 \wedge \cdots \wedge m_k = 0$ if $m_i = m_j$ for some $i \neq j$.

(2) Universal Property for Alternating Multilinear Maps.

If $\varphi : M \times \cdots \times M \to N$ is an alternating k-multilinear map then there is a unique R-module homomorphism $\Phi : \Lambda^k(M) \to N$ such that $\varphi = \Phi \circ \tau$, where $\tau : M \times \cdots \times M \to \Lambda^k(M)$ is the map defined by $\tau(m_1, \cdots, m_k) = m_1 \wedge \cdots \wedge m_k$.

Proof). (1) We show that $A(M) = \{ m_1 \otimes \cdots \otimes m_k \; ; \; \exists i, j \; (i \neq j \wedge m_i = m_j) \}$.

($\subset$) Manifestly

($\supset$) First, we note that for $m, m' \in M$

$$m' \otimes m = (m'+m) \otimes (m'+m) - (m' \otimes m' + m \otimes m' + m \otimes m)$$

$$\equiv - m \otimes m' \text{ modulo } A(M).$$

Thus, every $m_1 \otimes \cdots \otimes m_k$ with $m_i = m_j$ for some $i \neq j$ is equivalent to $m_1' \otimes \cdots \otimes m_{k-1}' \otimes m_{k-1}$

Thus, $m_1 \otimes \cdots \otimes m_k$ is in $A(M)$ if $m_i = m_j$ for some distinct i and j.

The second assertion is clear.

(2) It follows from TFDC and note that since φ is alternating, $\varphi' \tau = 0$.

$$\begin{array}{ccccc} \overset{\times}{\otimes}_k M & \hookrightarrow & T^k(M) & \xleftarrow{\tau} & A(M) \\ {\scriptstyle\varphi}\downarrow & \swarrow_{\varphi'} & & & \downarrow{\scriptstyle \operatorname{coker}\tau} \\ N & \xleftarrow{\Phi} & & & \Lambda^k(M) \end{array}$$

Cor37 Let V be a finite dimensional vector space over the field F with basis $\mathcal{B} = \{v_1, \cdots, v_n\}$. Then the vectors $v_{i_1} \wedge v_{i_2} \wedge \cdots \wedge v_{i_k}$ for $1 \le i_1 < i_2 < \cdots < i_k \le n$ are a basis of $\Lambda^k(V)$, and $\Lambda^k(V) = 0$ when $k > n$. In particular, $\dim(\Lambda^k(V)) = \binom{n}{k}$.

Proof) By the proof of thm 36(1), we have $m' \otimes m = -m \otimes m'$ modulo $A(V)$, i.e., $m' \wedge m = -m \wedge m'$ and by the result of thm 36(1) we have $m_1 \wedge \cdots \wedge m_k = 0$ iff $m_i = m_j$ for distinct i and j. Thus, $\mathcal{B}_k := \{v_{i_1} \wedge \cdots \wedge v_{i_k} ; 1 \le i_1 < \cdots < i_k \le n\}$ spans $\Lambda^k(V)$ and let n_k be the cardinal of $\mathcal{B}_k$.

Since, $k > n$ clearly $\Lambda^k(V) = 0$. Assume that $k \le n$ and we verify $\mathcal{B}_k$ is linearly independent.

Assume that $\mathcal{B}_k$ is not linearly independent, there exists nontrivial a_i such that $\sum_{1 \le i \le n_k} a_i w_i = 0$ where w_i is in $\mathcal{B}_k$ and let $a_1 \neq 0$ w.l.o.g. Define a map $f : V^k \to F$ which is given by the assignment of basis, $v_1 \wedge \cdots \wedge v_k \mapsto 1$, others $\mapsto 0$. Then clearly, f is alternating multilinear map so can be extend to $\varphi : \Lambda^k(V) \to F$. Then applying $\sum_{1 \le i \le n_k} a_i v_i = 0$ by φ, we obtain $a_1 = 0$, a contradiction.

Therefore, $\mathcal{B}_k$ is a basis of $\Lambda^k(V)$ and its cardinal is $\binom{n}{k}$.

Prop38 If φ is an endomorphism on an n-dimensional vector space V, then $\Lambda^n(\varphi)(w) = \det(\varphi) w$ for all $w \in \Lambda^n(V)$.

Proof) It is enough to show that D is the determinat function. By construction of $\Lambda^n(\varphi)$, D is clearly alternating multilinear and assign the identity the 1.

Prop39 Let σ be an element in the symmetric group S_k and let $\varepsilon(\sigma)$ be the sign of the permutation σ. Then

KOKUYO LOOSE-LEAF ✓ B26BT 6 mm ruled × 26 lines

(1) for every $\omega \in S^k(M)$ we have $\sigma\omega = \omega$, and

(2) for every $\omega \in \Lambda^k(M)$ we have $\sigma\omega = \varepsilon(\sigma)\omega$.

Proof) (1) By thm 34 (1)

(2) By the proof of thm 36 (1)

Prop40 Suppose $k!$ is a unit in the ring R and M is an R-module. Then

(1) The map $\frac{1}{k!}\mathrm{Sym}$ induces an R-module isomorphism between the kth symmetric power of M and the R-submodule of symmetric k-tensors: $\frac{1}{k!}\mathrm{Sym} : S^k(M) \approx \{\text{symmetric } k\text{-tensors}\}$.

(2) The map $\frac{1}{k!}\mathrm{Alt}$ induces an R-module isomorphism between the kth exterior power of M and the R-submodule of alternating k-tensors: $\frac{1}{k!}\mathrm{Alt} : \Lambda^k(M) \approx \{\text{alternating } k\text{-tensor}\}$.

Proof) (1) It suffice to show that $\ker\left(\frac{1}{k!}\mathrm{Sym}\right) = \mathcal{C}^k(M)$.

(2) Thm 34 (1) assert $m = m_1 \otimes \cdots \otimes m_k - m_{\sigma(1)} \otimes \cdots \otimes m_{\sigma(k)}$ is a generator of $\mathcal{C}^k(M)$ and since $\frac{1}{k!}\mathrm{Sym}$ is multilinear, and $\left(\frac{1}{k!}\mathrm{Sym}\right)(m) = 0$, we have the inclusion.

(3) Let $z \in T^k(M)$ with $\left(\frac{1}{k!}\mathrm{Sym}\right)(z) = 0$. Then we have $\frac{1}{k!}\sum_{\sigma\in S_k}(\sigma(z) - z) = \frac{1}{k!}\sum_{\sigma\in S_k}(-z)$. Since, by thm 34 (1), $\sigma z - z \in \mathcal{C}^k(M)$ for every σ. We have $z = \frac{1}{k!}\sum_{\sigma\in S_k}(-z) \in \mathcal{C}^k(M)$.

(2) It suffice to show that $\ker\left(\frac{1}{k!}\mathrm{Alt}\right) = \mathcal{A}^k(M)$.

Note that by the proof of prop40 (1) we have $m_1 \otimes m_2 \equiv m_2 \otimes m_1$ modulo $\mathcal{A}^k(M)$ so by induction, $z \equiv \varepsilon(\sigma)\sigma(z)$ modulo $\mathcal{A}^k(M)$

(2) It sufficient to shows for $m = m_1 \otimes \cdots \otimes m_k$ with $m_i = m_j$ for $i \neq j$, $\left(\frac{1}{k!}\mathrm{Alt}\right)(m) = 0$

$$\left(\frac{1}{k!}\mathrm{Alt}\right)(m) = \sum_{\sigma\in S_k} \varepsilon(\sigma)\,\sigma(m)$$

$$= \sum_{\sigma\in S_k|_2} \varepsilon(\sigma)\,\sigma(m) + \varepsilon((i_2)\sigma)\,(i_2)\circ\sigma\,(m)$$

$$= \sum \varepsilon(\sigma)\,\sigma(m) - \varepsilon(\sigma)\,\sigma(m)$$

$$= 0$$

(2) Let $z \in {}^2T^k(M)$ with $\left(\frac{1}{k!}\mathrm{Alt}\right)(z) = 0$.

Since $z = \frac{1}{k!}\sum_{\sigma\in S_k} z - \varepsilon(\sigma)\,\sigma(z)$, and $z - \varepsilon(\sigma)\,\sigma(z) \in \mathcal{A}^k(M)$ for every σ. Thus, $z \in \mathcal{A}^k(M)$.

KOKUYO LOOSE-LEAF ノ-836BT 6 mm ruled×36 lines

No.

Date

Thm1 Let R be a ring and let M be a left R-module. Then the following are equivalent.

(1) M is a Noetherian R-module.

(2) Every nonempty set of submodules of M contains a maximal element under inclusion.

(3) Every submodule of M is finitely generated.

Proof)

(1) $\Rightarrow$ (2) Let $\mathcal{A}$ be a non-empty collection of submodules of M. Suppose for every $N \in \mathcal{A}$ there exists $N' \in \mathcal{A}$ such that $N \subsetneq N'$. Then we obtain an increasing chain $N_0 \subsetneq N_1 \subsetneq \cdots \subsetneq N_n \subsetneq \cdots$. This contradicts M is Noetherian R-module.

Thus, $\exists N \in \mathcal{A}\ \forall N' \in \mathcal{A}\ ((\exists n \in N,\ n \notin N') \vee (\forall n' \in N'\ n' \in N))$ holds.

Then for $N'' \in \mathcal{A}$ such that $N \subseteq N''$, $N = N''$ holds. This assert N is maximal.

(2) $\Rightarrow$ (3) Let N be a submodule of M and let $\mathcal{B}$ be the collection of finitely generated submodule of N. Note that since $\{0\} \in \mathcal{B}$, $\mathcal{B}$ is not empty. (2) assert $\mathcal{B}$ has maximal B. If $B = N$ we're done. Suppose not, there exists $x \in N \setminus B$. Then we obtain another submodule B' which generated by B and x, and clearly B' is finitely generated. This contradicts B is maximal.

(3) $\Rightarrow$ (1) Let $M_0 \subseteq M_1 \subseteq \cdots$ be a chain of submodules of M, and $N := \cup M_i$ is the submodule of M. By (3), N is finitely generated, $N = \langle a_1, \cdots, a_n \rangle$. Since $a_j \in N = \cup M_i$ for every j, this implies $\forall j\ \exists i\ a_j \in M_i$ moreover, we pick i as inductivity, $\forall j\ \exists i\ \forall k \leq j\ a_k \in M_i$. Therefore, $\exists i\ \forall j\ a_j \in M_i$. Thus $M_i = N$ and M is Noetherian.

KOKUYO LOOSE-LEAF A-836BT 6 mm ruled 6×36 lines

Cor 2. If R is a P.I.D. then every nonempty set of ideals of R has a maximal element and R is a Noetherian ring.

Proof). By definition, every submodule of module R is an ideal. Then every submodule of P.I.D. R is finitely generated. Thus, we're done by previous theorem.

Prop3. Let R be an integral domain and let M be a free R-module of rank $n < \infty$. Then any $n+1$ elements of M are R-linearly dependent, i.e. for any $\gamma_1, \cdots, \gamma_{n+1} \in M$ there are elements $r_1, \cdots, r_{n+1} \in R$, not all zero, such that $r_1\gamma_1 + \cdots + r_{n+1}\cdot\gamma_{n+1} = 0$.

Proof). Let F be a quotient field induced by integral domain R.

Then, $M \cong R^{n\oplus} \subseteq F^{n\oplus}$ holds.

Now we assert $F^{n\oplus}$ is the F-module of rank n. (This fact is nontrivial.)

For every $\gamma_1, \cdots, \gamma_{n+1} \in M$, since $F^{n\oplus}$ is F-linearly independent, there exists $r_1, \cdots, r_{n+1} \in F$, such that $\sum_{1\le i\le n+1} r_i\gamma_i = 0$.

Now every $r_i \in F$ has the form $\frac{r_i'}{f_i}$ where $r_i' \in R$, $f_i \in R\setminus\{0\}$, we obtain

$$\sum_{1\le i\le n+1} \frac{r_i'}{f_i}\cdot\gamma_i = 0, \text{ moreover,}$$

$$\sum_{1\le i\le n+1} (f_1\cdots\hat{f_i}\cdots f_{n+1}\cdot r_i')\cdot\gamma_i = 0.$$

Now, $(f_1\cdots\hat{f_i}\cdots f_{n+1}\cdot r_i') \in R$ for every i.

Thus, $\exists\, r_1'', r_2'', \cdots, r_{n+1}'' \in R$, $\sum_{1\le i\le n+1} r_i''\cdot\gamma_i = 0$

Thm 4 Let R be a P.I.D., let M be a free R-module of finite rank n and let N be a submodule of M. Then

(1) N is free of rank m, $m \le n$ and

(2) there exists a basis $y_1, \cdots, y_n$ of M so that $a_1 y_1, \cdots, a_m y_m$ is a basis of N where $a_1, \cdots, a_m$ are nonzero elements of R with the divisibility relations $(a_m) \subset \cdots \subset (a_1)$.

Proof). If $N = 0$, both assertions are obvious. Let $N \neq 0$.

For $\varphi \in \mathrm{Hom}(M, R)$, $\varphi(N)$ is a submodule of R, since R is a P.I.D., for some $a_\varphi \in R$ $\varphi(N) = (a_\varphi)$.

$\mathcal{A} := \{ \varphi(N) ; \varphi \in \mathrm{Hom}(M, R) \}$.

Note that since $\mathrm{id} \in \mathrm{Hom}(M, R)$, $\mathcal{A}$ is not empty. By Cor 2. $\mathcal{A}$ has maximal element $v(N)$ and let a_1 be an element with $v(N) = (a_1)$.

First we assert a_1 is non-zero.

Let $x_1, \cdots, x_n$ be any basis of the free module M and let $\pi_i \in \mathrm{Hom}(M, R)$ be the natural projection.

Since $N \neq 0$, $\pi_i(N) \neq 0$ for some i, this assert $\mathcal{A}$ has non trivial module, (a_1) is not trivial, $a_1 \neq 0$. Now pick $y \in N$ as $v(y) = a_1$ then we assert $(\varphi(y)) \subset (a_1)$ for every $\varphi \in \mathrm{Hom}(M, R)$.

For $r_1, r_2 \in R$, let $\psi := r_1 v + r_2 \varphi \in \mathrm{Hom}(M, R)$ and let $d := r_1 a_1 + r_2 \varphi(y)$.

KOKUYO LOOSE-LEAF ノ-836BT 6mm ruled×36 lines

Then, $\psi(\mathfrak{y}) = (r_1\nu + r_2\varphi)(\mathfrak{y}) = (r_1\nu)(\mathfrak{y}) + (r_2\varphi)\mathfrak{y} = r_1 a_1 + r_2\varphi(\mathfrak{y}) = d$.

Thus, $d \in \psi(N)$ moreover, $(d) \subset \psi(N)$ And we have $(a_1) \subset (d)$ hence, $(a_1) \subset (d) \subset \psi(N)$. The maximality of (a) assert $(a) = \psi(N)$ moreover, $(a) = (d)$. Thus, for every $r_1, r_2 \in R$, $(a_1) = (r_1 a_1 + r_2\varphi(\mathfrak{y}))$ holds. Therefore, $(\varphi(\mathfrak{y})) \subset (a_1)$. This show for every projection π_i, $(\pi_i(\mathfrak{y})) \subset (a_1)$ holds. Thus, for every i there exists $b_i \in R$ such that $\pi_i(\mathfrak{y}) = b_i \cdot a$ and we define $\mathfrak{y}_1 = \sum_{1 \le i \le n} b_i \cdot x_i$. Note that, by definition, $a_1\mathfrak{y}_1 = \sum_i \pi_i(\mathfrak{y})\, x_i = \mathfrak{y}$.

Since, $a_1 = \nu(\mathfrak{y}) = \nu(a_1\mathfrak{y}_1) = a_1\nu(\mathfrak{y}_1)$ and a_1 is nonzero element in integral domain, $\nu(\mathfrak{y}_1) = 1$.

Now we assert we can pick $\mathfrak{y}_1$ as one element in a base for M and $a_1\mathfrak{y}_1$ as one element in a base for N. To show this assertion we prove following equations:

(a) $M = R\mathfrak{y}_1 \oplus \ker\nu$, and

(b) $N = Ra_1\mathfrak{y}_1 \oplus (N \cap \ker\nu)$.

First we verify (a). For $x \in M$. Since $\nu(x - \nu(x)\mathfrak{y}_1) = \nu(x) - \nu(x)\nu(\mathfrak{y}_1) = 0$, $x - \nu(x)\mathfrak{y}_1 \in \ker\nu$ and clearly $\nu(x)\mathfrak{y}_1 \in R\mathfrak{y}_1$ thus, $x \in R\mathfrak{y}_1 \oplus \ker\nu$. Conversely, for $r \in R$, $r\mathfrak{y}_1 = \sum_i (rb_i)\, x_i \in M$ and clearly $\ker\nu \subset M$ holds. Therefore $M = R\mathfrak{y}_1 \oplus \ker\nu$.

Next we verify (b). For $x \in N$. We obtain $x - \nu(x)\mathfrak{y}_1 \in \ker\nu$. Since $\nu(N) = (a_1)$, $\nu(x)\mathfrak{y}_1 \in \nu(N)\mathfrak{y}_1 = (a_1)\mathfrak{y}_1 = (\mathfrak{y}) \subset N$ thus, $x - \nu(x)\mathfrak{y}_1 \in N$ moreover, $x - \nu(x)\mathfrak{y}_1 \in N \cap \ker\nu$.

And by $\nu(N) = (a_1)$, $\exists b \in R$, $\nu(x) = b a_1$ holds, $\nu(x)\vartheta_1 = b a_1 \vartheta_1 \in R a_1 \vartheta_1$.

Therefore, $x = \nu(x)\vartheta_1 + (x - \nu(x)\vartheta_1) \in R a_1 \vartheta_1 \oplus (N \cap \ker \nu)$.

Conversely, for $r \in R$, $r a_1 \vartheta_1 = r y \in N$ thus, $R a_1 \vartheta_1 \oplus (N \cap \ker \nu) \subset N$. Therefore, $N = R a_1 \vartheta_1 \oplus (N \cap \ker \nu)$.

Now we prove (1) by induction on the rank m of N. If $m = 0$, then by definition of rank, $\forall n \in N\ \exists r \in R \setminus \{0\}$ $rn = 0$, since R is finitely generated, $n = 0$, $N = 0$ i.e. N is a free module.

Assume that $m > 0$. Note that $N \neq 0$. First we show the rank of $N \cap \ker \nu$ is $m-1$. Since, R is an integral domain, the rank of $R a_1 \vartheta_1$ is 1 and by Exercise 3, the rank of $N \cap \ker \nu$ is $m-1$. By assumption of induction, $N \cap \ker \nu$ is a free R-module of rank $m-1$.

Now, (b) assert every $n \in N$ has the form $r a_1 \vartheta_1 + \sum_{1 \le i \le m-1} r_i n_i$ where $\{n_i,\ 1 \le i \le m-1\} = N \cap \ker \nu$. Therefore N is free module of rank m, we proved (1).

Finally, we prove (2) by induction n, the rank of M. Since $\ker \nu$ is a submodule of M, by (1) $\ker \nu$ is a free module and by (a) and Exercise 3, the rank of $\ker \nu$ is $n-1$.

Now $N \cap \ker \nu$ is a submodule of $\ker \nu$ of rank $n-1$, then by assumption, there exists a basis $\vartheta_2, \cdots, \vartheta_n$ of $\ker \nu$ and $a_2, \cdots, a_m \in R$ such that $a_2 \vartheta_2, \cdots, a_m \vartheta_m$ is a basis of $N \cap \ker \nu$ and $(a_m) \subset \cdots \subset (a_2)$ hold.

To assert the relation holds for rank n, it is enough to show that $(a_2) \subset (a_1)$.

Let φ be an R-module homomorphism which assigh $\vartheta_1 \mapsto 1$, $\vartheta_2 \mapsto 1$, $\vartheta_i \mapsto 0$ $(i > 2)$.

KOKUYO LOOSE-LEAF A-836BT 6 mm ruled x 30 lines

Then $a_1 = \varphi(a_1 \cdot y_1) = \varphi(y) \in \varphi(N)$. This shows $(a_1) \subset \varphi(N)$ and by maximality of (a_1), $(a_1) = \varphi(N)$. Since $a_2 = \varphi(a_2 \cdot y_2) \in \varphi(N)$, we have $(a_2) \subset \varphi(N) = (a_1)$. This couple the proof of theorem.

Thm 5 Fundametal Theorem, Existence: Invarint Factor Form.

Let R be a P.I.D. and let M be a finitely generated R-module.

(1) Then M is isomorphic to the direct sum of finitely many cyclic modules. More precisely,

$$M \cong R^r \oplus R/(a_1) \oplus \cdots \oplus R/(a_m)$$

for some integer $r \geq 0$ and nonzero elements $a_1, a_2, \cdots, a_m$ of R which are not units in R and which satisfy the $(a_m) \subset \cdots \subset (a_1)$.

(2) M is torsion free iff M is free.

(3) In the decomposition in (1),

$$\mathrm{Tor}(M) \cong R/(a_1) \oplus \cdots \oplus R/(a_m).$$

In paticular M is a torsion module iff $r = 0$ and in this case the annihilator of M is the ideal (a_m).

Proof). Since M is finitely generated, let $\{x_1, \cdots, x_n\}$ be the smallest cardinal with $F(\{x_1, \cdots, x_n\}) = M$. Let R^n be the free R-module of rank n with basis $b_1, \cdots, b_n$ and define the R-module homomorphism π which assign the b_i the x_i for every i. Since π is surjective, by First Isomorphism Theorem for module, we have $R^n/\ker\pi \cong M$. Since $\ker\pi$ is a submodule of R^n, by thm 4, we can pick

a basis $\eta_1, \cdots, \eta_n$ of R^n and $a_1, \cdots, a_m \in R$ such that $a_1\eta_1, \cdots, a_m\eta_m$ is a basis of $\ker\pi$ and $(a_m) \subset \cdots \subset (a_1)$.

This assert, $M \cong R^n/\ker\pi = (R\eta_1 \oplus \cdots \oplus R\eta_n) \,/\, (Ra_1\eta_1 \oplus \cdots \oplus Ra_m\eta_m)$ ···· (*)

To define a map $\pi' : R\eta_1 \oplus \cdots \oplus R\eta_n \longrightarrow R/(a_1) \oplus \cdots \oplus R/(a_m) \oplus R^{n-m}$, first we verify the following statement.

$$\alpha_1\eta_i = \alpha_2\eta_i \Rightarrow \alpha_1 = \alpha_2 \qquad \text{for every } i.$$

Since R is a P.I.D., does not has zero divisor, $(\alpha_1 - \alpha_2)\eta_i = 0$ implies $\alpha_1 - \alpha_2 = 0$ or $\eta_i = 0$, but clearly $\eta_i \neq 0$ thus, $\alpha_1 = \alpha_2$.

Thus we can define π' as following assignment,

$$\alpha_1\eta_1 \oplus \cdots \oplus \alpha_n\eta_n \longmapsto \alpha_1 + (a_1) \oplus \cdots \oplus \alpha_m + (a_m) \oplus \alpha_{m+1} \oplus \cdots \oplus \alpha_n .$$

Then clearly π' is a surjective, R-module homomorphism.

We assert $\ker\pi' = Ra_1\eta_1 \oplus \cdots \oplus Ra_m\eta_m \oplus 0 \oplus \cdots \oplus 0$. ···· (**).

Since $\pi'(r_1a_1\eta_1 \oplus \cdots \oplus r_m a_m\eta_m \oplus 0 \oplus \cdots \oplus 0) = r_1a_1 + (a_1) \oplus \cdots \oplus r_m a_m + (a_m) \oplus 0 \oplus \cdots \oplus 0$

$$= 0 .$$

And for $\alpha_1\eta_1 \oplus \cdots \oplus \alpha_n\eta_n \in \ker\pi'$ then, $\alpha_1 \in (a_1), \cdots, \alpha_m \in (a_m), \alpha_{m+1} = 0, \cdots, \alpha_n = 0$.

moreover, $\alpha_1 \in Ra_1, \cdots, \alpha_m \in Ra_m, \alpha_{m+1} = 0, \cdots, \alpha_n = 0$. Thus, $\ker\pi' \subset Ra_1\eta_1 \oplus \cdots \oplus Ra_m\eta_m$.

Therefore (**) holds and by (*), $M \cong R^n/\ker\pi \cong R/(a_1) \oplus \cdots \oplus R/(a_m) \oplus R^{n-m}$ holds.

If for some i, a_i is an unit, since R is a P.I.D. $(a_i) = R$, $R/(a_i) = 0$. Some can

KOKUYO LOOSE-LEAF A-806BT 6 mm ruled 36 lines

remove $R/(a_i)$ from decomposition. Let r be a integer $n-m$ then we obtain the relation

$M \simeq R^r \oplus R/(a_1) \oplus \cdots \oplus R/(a_m)$ with $(a_m) \subset \cdots \subset (a_1)$ we, complete the proof (1).

Since, $R/(a)$ is a torsion R-module for every non-zero element a in R.

Then, $\mathrm{Tor}(M) = \{ m \in M ; \exists r \in R \setminus \{0\}, rm = 0 \}$

$= 0 \oplus R/(a_1) \oplus \cdots \oplus R/(a_m)$ ···· (***)

thus, M is torsion free $\Leftrightarrow M \simeq R^r$, we proved (2), and by (***) if M is torsion module, $R/(a_1) \oplus \cdots \oplus R/(a_m) \simeq R^r \oplus R/(a_1) \oplus \cdots \oplus R/(a_m)$ thus, $r = 0$ and conversely, if $r = 0$ clearly M is torsion module. Finally $\mathrm{Ann}(M) = \bigcap_{1 \le i \le m} (a_i) = (a_m)$. Thus we complete the (3).

Thm 6. Fundamental Theorem, Existence : Elementary Divisor Form.

Let R be a P.I.D. and let M be a finitely generated R-module. Then M is the direct sum of a finite number of cyclic modules whose annihilators are either (0) or generated by powers of prime in R, i.e.,

$$M \simeq R^r \oplus R/(p_1^{\alpha_1}) \oplus \cdots \oplus R/(p_t^{\alpha_t})$$

where $r \ge 0$ is an integer and $p_1^{\alpha_1}, \cdots, p_t^{\alpha_t}$ are positive powers of (not necessarily distinct) primes in R.

Proof). For $a \in R$, since every P.I.D. is U.F.D., we obtain the factorization

$$a = u \cdot p_1^{\alpha_1} \cdot \cdots \cdot p_n^{\alpha_n} \quad \cdots (*)$$

where u is a unit, every p_i is irreducible and $(\forall i, j \; \exists u' \in R^\times, \; p_i = u' \cdot p_j \Rightarrow i = j)$ holds.

Then clearly we obtain the unique collection $\{(p_i^{d_i}); 1 \le i \le n\}$. Now we assert if $i \neq j$, $(p_i^{d_i})$ and $(p_j^{d_j})$ are comaximal.

Since every prime p_i are distinct, the greatest common divisor of p_i and p_j is 1 so is $p_i^{d_i}$ and $p_j^{d_j}$ if $i \neq j$.

Now, an ideal $(p_i^{d_i}) \cap (p_j^{d_j})$ is generated by greatest common divisors, 1, thus, $(p_i^{d_i}) \cap (p_j^{d_j}) = R$.

Therefore, $(p_i^{d_i}) + (p_j^{d_j}) = R$, comaximal, $i \neq j$.

Now, by (*), $(a) = (p_1^{d_1}) \cdot (p_2^{d_2}) \cdots (p_n^{d_n})$ holds and every distinct i and j, $(p_i^{d_i})$ and $(p_n^{d_n})$ are comaximal, then by Chinese Remainder Theorem,

$$R/(a) \cong R/(p_1^{d_1}) \times \cdots \times R/(p_n^{d_n}),$$

moreover, $R/(a) \cong R/(p_1^{d_1}) \oplus \cdots \oplus R/(p_n^{d_n})$ .... (**)

Therefore by thm 5 and (**) for a finitely generated module M,

$M \cong R^r \oplus R/(p_1^{d_1}) \oplus \cdots \oplus R/(p_n^{d_n})$, and

annihilator of R^r is 0 and $R/(p_i^{d_i})$ is $(p_i^{d_i})$. This couple the proof.

Thm 7 The Primary Decomposition Theorem.

Let R be a P.I.D. and let M be a nonzero torsion R-module with nonzero annihilator a. Suppose the factorization of a into distinct prime powers in R is $a = u p_1^{d_1} \cdots p_n^{d_n}$ and let $N_i = \{x \in M ; p_i^{d_i} x = 0\}$, $1 \le i \le n$. Then N_i is a submodule of M with annihilator $p_i^{d_i}$ and is

KOKUYO LOOSE-LEAF

the submodule of M of all elements annihilated by some power of p_i. We have $M = N_1 \oplus \cdots \oplus N_n$. If M is finitely generated then each N_i is the direct sum of finitely many cyclic modules whose annihilators are divisors of $p_i^{d_i}$.

Proof). First, we show $M = N_1 + \cdots + N_n$. Let $x \in M$, since a is an annihilator of M, $ax = 0$. Since $a = u \cdot p_1^{d_1} \cdots p_n^{d_n}$ we obtain $u(p_1^{d_1} \cdots p_n^{d_n})x = 0$ moreover, $(p_1^{d_1}x) \cdot \cdots \cdot (p_n^{d_n}x) = 0$. Since R is an integral domain, $\exists i$, $p_i^{d_i}x = 0$.

Thus, $x \in N_i \subseteq N_1 + \cdots + N_n$.

Next, we show $\{0\} = N_1 \cap \cdots \cap N_n$. or $n = 0$. Let $x \in N_0 \cap \cdots \cap N_n$. Then for $i \neq j$, $p_i^{d_i}x = 0 = p_j^{d_j}x$ thus, $(p_i^{d_i} - p_j^{d_j})x = 0$ and therefore $x = 0$.

Hence, $M = N_1 \oplus \cdots \oplus N_n$.

The secound assertion is by thm 6.

Thm 8. Let R be a P.I.D. and let p be a prime in R. Let F denote the field $R/(p)$.

(1) Let $M = R^r$. Then $M/pM \cong F^r$.

(2) Let $M = R/(a)$ where a is a nonzero element of R. Then

$$M/pM = \begin{cases} F & \text{if } (a) \subset (p) \\ 0 & \text{if } (a) \not\subset (p). \end{cases}$$

(3) Let $M = R/(a_1) \oplus \cdots \oplus R/(a_k)$ where $(a_i) \subset (p)$ for each i.

Then $M/pM \cong F^k$.

Proof). There exists a natural map from R^r into $(R/(p))^r$ which assign the $(d_1, \cdots, d_r)$ the $(d_1+(p), \cdots, d_n+(p))$. This map is clearly surjective R-module homomorphism and its kernel is pR^r.

(2) First we assert for a natural map $R \to R/(a)$; $r \mapsto r+(a)$ the image of (p) is

$$pM = p(R/(a)) = ((p)+(a))/(a).$$

Now since R is P.I.D., if $(a) \subset (p)$, $(p)+(a) = (p)$ and if $(a) \not\subset (p)$, $(p)+(a) = R$. Thus,

$$pM = \begin{cases} (p)/(a) & \text{if } (a) \subset (p) \\ R/(a) & \text{if } (a) \not\subset (p) \end{cases}$$

Moreover, by third isomorphism theorem,

$$M/pM = \begin{cases} (R/(a))/(p)/(a) = R/(p) = F. & \text{if } (a) \subset (p) \\ R/(a)/R/(a) = 0 & \text{if } (a) \not\subset (p) \end{cases}$$

(3) Clearly by (2).

Thm 9 Fundamental Theorem, Uniqueness

Let R be a P.I.D.

(1) Two finitely generated R-modules M_1 and M_2 are isomorphic iff they have the same free rank and the same list of invariant factors.

(2) Two finitely generated R-modules M_1 and M_2 are isomorphic iff they have the same

KOKUYO LOOSE-LEAF A-836BT 6 mm ruled×36 lines

free rank and the same list of elementary divisors.

Proof). If M_1 and M_2 have the same rank and list of invariant factors or the list of elementary divisors, it is clearly M_1 and M_2 are isomorphic.

Thus, we suppose $M_1 \approx M_2$.

First we show the free rank of M_1 and M_2 are the same. Since $M_1 \approx M_2$, $\mathrm{Tor}(M_1) \approx \mathrm{Tor}(M_2)$. Thus we obtain $R^{r_1} \approx M_1/\mathrm{Tor}(M_1) \approx M_2/\mathrm{Tor}(M_2) \approx R^{r_2}$ where r_1 and r_2 are free rank of M_1 and M_2 respectively.

Let p be any nonzero prime in R. We obtain $R^{r_1}/pR^{r_1} \approx R^{r_2}/pR^{r_2}$. By (1) of the previous lemma, $F_1^{r_1} \approx F_1^{r_2}$ where $F_1 = R/pR$.

Since the dimension of vector space is unique, $r_1 = r_2$. Thus the free rank of M_1 and M_2 are the same.

To assert the list of elementary divisors of M_1 and the list of elementary divisors of M_2 are the same, it is enough to show that the case of every elementary divisor of M_1 is the power of fixed prime p, and since $M_1 \approx M_2$ every elementary divisor of M_2 is the power of p. Thus we fixed a prime p.

Since the p-primary module of M_1 and M_2 has an annihilator, power of p. To assert the list of elementary divisors, it is enough to show the case of free rank of M_1 and M_2 are 0 i.e. M_1 and M_2 has an annihilator power of p.

Suppose that the power of p is an annihilator of M_1 and M_2. We proved by induction on the power of p in the annihilator of M_1 and M_2.

If power is 0, $\{0\} = M_1 \cong M_2$, we're done.

If not. Suppose that the elementary divisors of M_1 and M_2 are given by

$$M_1 : \underbrace{p, \cdots, p}_{m\text{-times}}, p^{d_1}, \cdots, p^{d_s},$$

where $2 \le d_1 \le \cdots \le d_s$ i.e. M_1 is the direct sum of cyclic modules with generators $x_1, \cdots, x_m, x_{m+1}, \cdots, x_{m+s}$, says, whose annihilators are $(p), \cdots, (p), (p^{d_1}), \cdots, (p^{d_s})$ respectively.

Now, the submodule pM_1 is the direct sum of cyclic modules with generators $px_1, \cdots, px_m, px_{m+1}, \cdots px_{m+s}$ with annihilators $(1), \cdots, (1), (p^{d_1-1}), \cdots, (p^{d_s-1})$ respectively.

Thus the elementary divisors of pM_1 are given by,

$$pM_1 : p^{d_1-1}, \cdots, p^{d_s-1}.$$

Similarly, suppose the elementary divisors of M_2 are given by

$$M_2 : \underbrace{p, \cdots, p}_{n\text{-times}}, p^{\beta_1}, \cdots, p^{\beta_t}$$

where $2 \le \beta_1 \le \cdots \le \beta_t$. Then the elementary divisors of pM_2 given by

$$pM_2 : p^{\beta_1-1}, \cdots, p^{\beta_t-1}.$$

Since, $M_1 \cong M_2$, $pM_1 \cong pM_2$ and the power of p in the annihilator of pM_1 is

KOKUYO LOOSE-LEAF

less than the power of p in the annihilator of M_1, then by induction, the list of elementary divisors of pM_1 and pM_2 are the same, i.e., $s-1 = t-1$ and $d_i - 1 = \beta_i - 1$ for all i so is $s=t$ and $d_i = \beta_i$ for $1 \le i \le s$.

Finally since $M_1/pM_1 \approx M_2/pM_2$, (3) of lemma 8 assert, $F^{m+s} \approx M_1/pM_1 \approx M_2/pM_2 \approx F^{n+t}$. This show that $m+s = n+t$ moreover, $m=n$.

Therefore, the list of elementary divisors of M_1 and the list of elementary divisors are the same. This comple the proof of (1).

Next, we prove (2).

Let $(a_m) \subset \cdots \subset (a_1)$ are invariant factors of M_1. Then modifying thm 6, we obtain the elementary divisors and we assert the largest invariant factors of M_1, a_m, is the product of the largest of the distinct prime power of elementary divisors, the secound invariant factors of M_1, a_{m-1}, is the product of the secound largest of the distinct prime of elementary divisors, and so on.

If $(b_n) \subset \cdots \subset (b_1)$ are invariant factors of M_2, we similarly obtain the elementary divisors.

Now the list of elementary divisors are the same, so is the list of invariant factors. This complete the proof of (2).

Prop12. The following are equivalent.

(1) λ is an eigenvalue of T.

(2) $\lambda I - T$ is a singular linear transformation of V.

(3) $\det(\lambda I - T) = 0$.

Proof) Let T be F-module endomorphism

(1) $\Rightarrow$ (2).

We prove the contraposition. If $\lambda I - T$ is a nonsingular, we have $\ker(\lambda I - T) = 0$. Thus, for every $v \in V$, $(\lambda I - T)(v) = 0$ implies $v = 0$. This assert λ is not an eigenvalue.

(2) $\Rightarrow$ (3)

We prove the contraposition. If $\det(\lambda I - T) = 0$, since F is a field, $\det(\lambda I - T)$ is a unit. Then by thm 11.30, $(\lambda I - T)$ is a unit in hom-set, isomorphism. So by Cor11.9, we obtain $\ker(\lambda I - T) = 0$.

(3) $\Rightarrow$ (1)

We prove the contradiction. Since for every $\lambda \in F$, $\lambda 0 = T(0)$ holds, if λ is not an eigenvalue of F, $\lambda v = T(v)$ implies $v = 0$. Thus, $\ker(\lambda I - T) = 0$.

Prop13. The minimal polynomial $m_T(x)$ is the largest invariant factor of V. All the invariant factors of V divide $m_T(x)$.

Proof) Let T be a fixed F-module endomorphism with n-dimensional F-module V.

By thm 10.5, since V is finite dimension, we have $V \approx F[x]/(a_1(x)) \oplus \cdots \oplus F[x]/(a_m(x))$ with $(a_1(x)) \supset \cdots \supset (a_m(x))$. And by condition (3), we have $\mathrm{Ann}(V) = (a_m(x))$.

Prop 1 The charastristic of a field F, $ch(F)$, is either 0 or a prime. If $ch(F) = p$ then for any $\alpha \in F$, $p \cdot \alpha = 0$

Proof). Assume that $ch(F)$, n, exists. For $n = a \cdot b$ we have $0 = n \cdot 1_F = (a \cdot 1_F)(b \cdot 1_F)$. Since F is an integral domain, $a \cdot 1_F = 0$ w.l.o.g. Thus we have $n \le a$. And clearly we have $a \le n$. so $n = a$, b is an units and a irreducible since F is a P.I.D.. Therefore n is a prime.

Let $ch(F) = p$, then $p \cdot \alpha = \underbrace{(\alpha + \cdots + \alpha)}_{p\text{-times}} = \alpha(1 + \cdots + 1) = \alpha \cdot 0 = 0$.

Prop 2. Let $\varphi : F \to F'$ be a homomorphism of fields. Then φ is either identically 0 or is injective, so that the image of φ is either 0 or isomorphic to F.

Thm 3 Let F be a field and let $p(x) \in F[x]$ be an irreducible polynomial. Then there exists a field K containing an isomorphic copy of F in which $p(x)$ has a root.

Proof) Let $K := F[x]/(p(x))$. Since, $p(x)$ is a irreducible, prime in $F[x]$ so $(p(x))$ is a maximal ideal. Thus, K is a field.

Let $\pi : F[x] \to K$, $f(x) \mapsto f(x) + (p(x))$. Now, $\pi|_F$ is a field homomorphism and $\pi|_F(1_F) = 1_F + (p(x))$ so $\pi|_F \neq 0$. By prop 2. $F \approx \pi|_F(F) \subseteq K$.

Next we show $\pi(x)$ is a root of $p(x)$.

Since, $\pi(p(x)) = \pi(a_n x^n + \cdots + a_0)$

$= \pi(a_n) \cdot \pi(x^n) + \cdots + \pi(a_0)$

$\approx a_n \cdot \pi(x^n) + \cdots + a_0 = p(\pi(x))$.

KOKUYO LOOSE-LEAF A-836BT 6mm ruled x 30 Pads

Thus we have, $p(\pi(x)) = \pi(p(x)) = 0 + (p(x))$. Thus, $p(x)$ has a root $\pi(x)$ in k

Thm 4. Let $p(x) \in F[x]$ be an irreducible polynomial of degree n over the field F and let K be the field $F[x]/(p(x))$. Let $\theta = x \bmod (p(x)) \in K$. Then the elements $1, \theta, \cdots, \theta^{n-1}$ are a basis for K as a vector space over F, so the degree of the extension is n, i.e., $[K : F] = n$.

Hence $K = \{a_0 + a_1\theta + \cdots + a_{n-1}\cdot\theta^{n-1} \; ; \; a_0, a_1, \cdots, a_{n-1} \in F\}$ consists of all polynomials of degree $< n$ in θ.

Proof) First we show $\{1, \theta, \cdots, \theta^{n-1}\}$ spans K. Let $a(x) \in F[x]$ and let $\pi : F[x] \to k$ be a natural map. Since, $F[x]$ is an Euclidean domain there exists $q(x)$ and $r(x)$ in $F[x]$ such that $a(x) = q(x)\cdot p(x) + r(x)$ with $\deg(r(x)) < \deg(p(x))$ or $r(x) = 0$.

Now, $a(x) + (p(x)) = r(x) + (p(x))$

$$= \sum_{0\le i\le n} a_i x^i + (p(x))$$

$$= \sum_{0\le i\le n} (a_i + (p(x)))(x^i + (p(x)))$$

$$= \sum_{0\le i\le n} (a_i + (p(x)))\cdot\theta^i.$$

Thus, $\{1, \cdots, \theta^{n-1}\}$ spans k.

Next, we verify $\{1, \cdots, \theta^{n-1}\}$ are linearly independent. Let $b_0 + b_1\theta + \cdots + b_{n-1}\theta^{n-1} = 0 + (p(x))$ then $b_1 + b_1 x + \cdots + b_{n-1}\cdot x^{n-1} \in (p(x))$. Thus, for some $q(x)$, $\sum_{0\le i\le n-1} b_i x^i = q(x)\cdot p(x)$.

If $q(x) = 0$, we're done. Assume $q(x) \neq 0$. If $b_i \neq 0$ for some i, $n-1 \ge \deg\left(\sum_{0\le i\le n-1} b_i x^i\right)$ $= \deg(q(x)\cdot p(x)) = \deg(q(x)) + \deg(p(x)) \ge n$ a contradiction thus we have $b_i = 0$ for every i.

Therefore, $\{1, \cdots, \theta^{n-1}\}$ are linearly independent, is a basis of K.

Cor 5. Let K be as in thm 4, and let $a(\theta), b(\theta) \in K$ be two polynomials of degree $< n$ in θ. Then addition in K is defined simply by usual polynomial addition and multiplication in K is defined by $a(\theta) \cdot b(\theta) = r(\theta)$ where $r(x)$ is the remainder (of degree $< n$) obtained dividing the polynomial $a(x) \cdot b(x)$ by $p(x)$ in $F[x]$.

Proof) Let $+_\theta$ and $\times_\theta$ be given addition and multiplication. Let $a(\theta) = a_0 + \cdots + a_{n-1}\theta^{n-1}$, $b(\theta) = b_0 + \cdots + b_{n-1}\theta^{n-1}$ and let $a(x), b(x) \in F[x]$ with $a(\theta) = a(x) + (p(x))$, $b(\theta) = b(x) + (p(x))$ respectively. Since $F[x]$ is a Euclidean domain, let $q(x)$ and $r(x)$ be $a(x) \cdot b(x) = q(x) \cdot p(x) + r(x)$ with $\deg(r(x)) < \deg(p(x))$ or $r(x) = 0$.

$$\begin{aligned} a(\theta) + b(\theta) &= \big(a(x) + (p(x))\big) + \big(b(x) + (p(x))\big) \\ &= \big(a(x) + b(x)\big) + (p(x)) \\ &= a(\theta) +_\theta b(\theta). \end{aligned}$$

$$\begin{aligned} a(\theta) \cdot b(\theta) &= \big(a(x) + (p(x))\big) \cdot \big(b(x) + (p(x))\big) \\ &= a(x)\, b(x) + (p(x)) \\ &= q(x) \cdot p(x) + r(x) + (p(x)) \\ &= r(\theta). \end{aligned}$$

Thm 6 Let F be a field and let $p(x) \in F[x]$ be an irreducible polynomial. Suppose K is an extension field of F containing a root α of $p(x)$: $p(\alpha) = 0$. Let $F(\alpha)$ denote the subfield of K generated over F by α.

Then $F'(\alpha) \simeq F'[x]/(p(x))$.

Proof) Let $\varphi : F'[x] \to F'(\alpha)$; $a(x) \to a(\alpha)$ the this is a field morphism.

Now we assert $\ker \varphi = (p(x))$. Since $p(\alpha) = 0$ we have $\alpha \in \ker \varphi$ so we have $(p(x)) \subset \ker \varphi$. And since $(p(x))$ is maximal we obtain either $(p(x)) = \ker \varphi$ or $\ker \varphi = F'[x]$. If $\ker \varphi = F'[x]$, by First Isomorphism Theorem we have $0 = F'[x]/\ker \varphi \simeq F'(\alpha)$, a contradiction.

Thus, we have $\ker \varphi = (p(x))$, $F'(\alpha) \simeq F'[x]/(p(x))$.

Cor 7. Suppose in theorem 6 that $p(x)$ is of degree n. Then

$F'(\alpha) = \{ a_0 + a_1 \alpha + a_2 \cdot \alpha^2 + \cdots + a_{n-1} \cdot \alpha^{n-1} \; ; \; a_0, \cdots, a_{n-1} \in F' \} \subseteq K$.

Proof) By thm 4 and thm 6.

Thm 8 Let $\varphi : F \xrightarrow{\sim} F'$ be an isomorphism of fields. Let $p(x) \in F[x]$ be an irreducible polynomial and let $p'(x) \in F'[x]$ be the irreducible polynomial obtainted by applying the map φ to the coefficients of $p(x)$. Let α be a root of $p(x)$ (in some extension of F) and let β be a root of $p'(x)$ (in some extension of F'). Then there is an isomorphism $\sigma : F(\alpha) \to F'(\beta)$; $\alpha \mapsto \beta$ mapping α to β and extending φ, i.e., such that σ restricted to F is the isomorphism φ.

Proof). By assumption the map $\Phi : F[x]/(p(x)) \to F'[x]/(p'(x))$; $\sum_{0 \le i \le n} a_i x^i + (p(x)) \mapsto \sum_{0 \le i \le n} \varphi(a_i) x^i + (p'(x))$ is an field isomorphism. And by thm 6 we obtain $F(\alpha) \simeq F'(\beta)$ and the restriction is the isomorphism φ.

Prop 9. Let α be algebraic over F. Then there is a unique monic irreducible polynomial $m_{\alpha,F}(x) \in F[x]$ which has α as a root. A polynomial $f(x) \in F[x]$ has α as a root $\Leftrightarrow$ $m_{\alpha,F}(x)$ divides $f(x)$ in $F[x]$.

Proof). First we show the first assertion.

Since α is algebraic over F, there exists polynomial $g(x) \in F[x]$ with $g(\alpha) = 0$. We may assume that $g(x)$ is monic and minimal degree. Suppose $g(x)$ is reducible then there exists $a(x), b(x) \in F[x] \setminus F$ such that $g(x) = a(x) \cdot b(x)$. Then we have $0 = g(\alpha) = a(\alpha) \cdot b(\alpha)$ and since F is an integral domain, $a(\alpha) = 0$ w.l.o.g. this contradicts the minimality of degree of $g(x)$.

Assume that there exists monic irreducible polynomial $f(x)$ with root α. Then since $F[x]$ is a Euclidean domain, there exists $q(x)$ and $r(x)$ in $F[x]$ such that $f(x) = q(x) \cdot g(x) + r(x)$ with $\deg(g(x)) > \deg(r(x))$ or $r(x) = 0$. Since we have $r(\alpha) = 0$ and by minimality of degree of $g(x)$ we obtain $r(x) = 0$, $f(x) = q(x) \cdot g(x)$. Since, $f(x)$ is irreducible we have $q(x)$ is an unit and since both $f(x)$ and $g(x)$ are monic, $q(x) = 1$. Therefore $f(x) = g(x)$.

The secound assertion is by proof in first assertion and conversely is clear.

Cor 10. If L/F is an extension of fields and α is algebraic over both F and L, then $m_{\alpha,L}(x)$ clivides $m_{\alpha,F}(x)$ in $L[x]$.

Proof) Since $m_{\alpha,F}(x) \in F[x] \subset L[x]$. by secound assertion in prop 9, we obtain $m_{\alpha,L}(x)$ divides $m_{\alpha,F}(x)$.

Prop11 Let α be algebraic over the field F_1 and let $F_1(\alpha)$ be the field generated by α over F_1. Then $F_1(\alpha) \simeq F_1[x]/(m_\alpha(x))$ so that in particular $[F_1(\alpha) : F_1] = \deg m_\alpha(x) = \deg \alpha$, i.e., the degree of α over F_1 is the degree of the extension it generates over F_1.

Proof) The first assertion is by thm 6 and the second assertion is by thm 4 and thm 6.

Prop12 The element α is algebraic over F_1 iff the simple extension $F_1(\alpha)/F_1$ is finite. More precisely, if α is an element of an extension of degree n over F_1 then α satisfies a polynomial of degree at most n over F_1 and if α satisfies a polynomial of degree n over F_1 then the degree of $F_1(\alpha)$ over F_1 is at most n.

Proof) $\Rightarrow$) Suppose that α is a root of $f(x) \in F_1[x]$ with $\deg(f(x)) = n$. By prop 11 and the second assertion in prop 9, $[F_1(\alpha) : F_1] = \deg(m_\alpha(x)) \leq \deg(f(x)) = n$.

$\Leftarrow$) Let $\alpha \in K$ with $F_1 \subseteq K$ and $[K : F_1] = n$. Then since $1, \alpha, \cdots, \alpha^n$ are linearly dependent over F_1, we have $b_0, \cdots, b_n \in F_1$ such that $b_0 + \cdots + b_n \alpha^n = 0$ and not every b_i is not the zero. This show that $b_n x^n + \cdots + b_0$ is nonzero polynomial with root α and the degree of this polynomial is at most n.

Cor 13 If the extension K/F_1 is finite, then it is algebraic.

Proof). Let $\alpha \in K$. Since $F_1(\alpha)$ is a subspace of K over F_1. So $\dim F_1(\alpha) \leq \dim K$ i.e. $[F_1(\alpha) : F_1] \leq [K : F_1]$. By assumption $[K : F_1]$ is finite, hence so is $[F_1(\alpha) : F_1]$ and by prop 12 α is algebraic.

Thm 14. Let $F \subseteq K \subseteq L$ be fields. Then $[L : F] = [L : K] \cdot [K : F]$, i.e. extension degrees are multiplicative, where if one side of the equation is infinite, the other side is also infinite.

Proof) First, suppose that $[L : K] = m$ and $[K : F] = n$ are finite.

Let $\{\alpha_1, \cdots, \alpha_m\}$ be a basis for L over K and $\{\beta_1, \cdots, \beta_n\}$ be a basis for K over F. We assert $\{\alpha_i \cdot \beta_j \mid 1 \le i \le m, 1 \le j \le n\}$ be a basis of L over F. For arbitrary $\ell \in L$ there exists $a_1, \cdots, a_m \in K$ with $\ell = \sum_{1 \le i \le m} a_i \cdot \alpha_i$ and for every $a_i \in K$ there exists $b_{i1}, \cdots, b_{in} \in F$ such that $a_i = \sum_{1 \le j \le m} b_{ij} \beta_j$. Thus we have $\ell = \sum_{1 \le i \le m} \sum_{1 \le j \le n} b_{ij} \cdot \alpha_i \beta_j$ so, $\{\alpha_i \cdot \beta_j\}$ spans L. For $c_{ij} \in F$ with $\sum_{1 \le i \le m} \sum_{1 \le j \le n} c_{ij} \cdot \alpha_i \beta_j = 0$. Let $\alpha_i = \sum_{1 \le j \le n} c_{ij} \beta_j$ then we have $\sum_{1 \le i \le m} a_i \alpha_i = 0$ so $a_i = 0$ for every i and therefore $c_{ij} = 0$ for every i and j. Therefore $\{\alpha_i \cdot \beta_j\}$ is a basis of L over F, $[L : F] = m \cdot n = [L : K] \cdot [K : F]$.

Finally we consider the infinite cases.

If $[K : F]$ is infinite. Then since we have $\dim K < \dim L$, $[L : F]$ is also infinite.

If $[L : K]$ is infinite. There exists infinitely many elements in L which are linearly independent over K. This collection is also linearly independent over F. Thus $[L : F]$ is infinite.

If $[L : F]$ is infinite. Think the contraposition for finite case.

Cor 15. Suppose L / F is finite extension and let K be any subfield of L containing F, $F \subseteq K \subseteq L$. Then $[K : F]$ divides $[L : F]$.

Proof) Derived from thm 14.

No.

Date

Lemma 16. $F(\alpha,\beta) = F(\alpha)(\beta)$, i.e., the field generated over F by α and β is the field generated by β over the field $F(\alpha)$ generated by α.

Proof) ($\subseteq$) Since $F \subseteq F(\alpha) \subseteq F(\alpha)(\beta)$, $\alpha \in F(\alpha)(\beta)$ and $\beta \in F(\alpha)(\beta)$. Then by minimality of $F(\alpha,\beta)$ we have $F(\alpha,\beta) \subseteq F(\alpha)(\beta)$.

($\subseteq$) Since $F \subseteq F(\alpha,\beta)$ and $\alpha \in F(\alpha,\beta)$, by minimality we have $F(\alpha) \subseteq F(\alpha,\beta)$, and since $\beta \in F(\alpha,\beta)$, we have $F(\alpha)(\beta) \subseteq F(\alpha,\beta)$.

Thm 17. The extension K/F is finite iff K is generated by a finite number of algebraic elements over F. More precisely, a field generated over F by a finite number of algebraic elements of degree $n_1, \cdots, n_k$ is algebraic of degree $\leq n_1 n_2 \cdots n_k$.

Proof) First, we show the first assertion. Let $[K:F] = n$ and let $\{\alpha_1, \cdots, \alpha_n\}$ be a basis of K over F. Since $F \subseteq F(\alpha_i) \subseteq K = \{\sum_{1 \leq i \leq n} a_i \alpha_i \; ; \; a_i \in F\}$, by Cor 15, $[F(\alpha_i):F]$ divides $[K:F]$. Then by Cor 13, every α_i is algebraic over F. Since K is generated by $\alpha_1, \cdots, \alpha_n$ over F, we have the result. Conversely derived from the secound assertion.

Now, we verify the secound assertion. Let $\alpha_1, \cdots, \alpha_n$ be algebraic over F of degree $n_1, \cdots, n_k$ respectively. Then by thm 14, $[K:F] = [F_k:F_{k-1}] \cdot [F_{k-1}:F_0] = [F_k:F_{k-1}] \cdots [F_1:F_0] \leq [F_k:F] \cdots [F_1:F] = n_1 \cdots n_k$. And by Cor 13, K is algebraic.

Cor 18 Suppose α and β are algebraic over F. Then $\alpha \pm \beta$, $\alpha\beta$, α/β (for $\beta \neq 0$), are all algebraic.

Proof) Since, α and β are algebraic over F, by thm 17, the extension $F(\alpha,\beta)/F$ is finite, by cor 13,

$F(\alpha,\beta)$ is algebraic. Since all of $\alpha\pm\beta$, $\alpha\beta$, $\frac{\alpha}{\beta}$ are in $F(\alpha,\beta)$, they are algebraic.

Cor 19. Let L/F be an arbitrary extension. Then the collection of elements of L that are algebraic over F from a subfield K of L.

Proof) By cor 18, the set of algebraic is closed under the operations on the field.

Thm 20. If K is algebraic over F and L is algebraic over K, then L is algebraic over F.

Proof). Let $\alpha\in L$. Since L is algebraic over K, there is a polynomial $\sum_{1\le i\le n} a_i\cdot x^i \in K[x]$ with $\sum_{1\le i\le n} a_i\cdot\alpha^i = 0$. For the field $F(\alpha, a_0,\cdots,a_n)$, by thm 17, the extension $F(\alpha,a_0,\cdots,a_n)/F$ is finite, and by prop 9, $\deg(m_{\alpha,F(a_0,\cdots,a_n)}) \le \deg(\sum_{0\le i\le n} a_i\,x^i) = n$. Thus, by lemma 16,

$$[F(\alpha,a_0,\cdots,a_n):F] = [F(\alpha,a_0,\cdots,a_n):F(a_0,\cdots,a_n)]\cdot[F(a_0,\cdots,a_n):F]$$
$$= \deg(m_{\alpha,F(a_0,\cdots,a_n)})\cdot(\text{finite}) = (\text{finite}).$$

Then by thm 17, $F(\alpha,a_0,\cdots,a_n)$ is an algebraic extension over F, in paticular, α is algebraic.

Prop 21. Let K_1 and K_2 be two extensions of a field F contained in K. Then $[K_1K_2:F]\le [K_1:F]\cdot[K_2:F]$ with equality iff an F-basis for one of the fields remains linearly independent over the other field. If $\alpha_1,\cdots,\alpha_n$ and $\beta_1,\cdots,\beta_m$ are bases for K_1 and K_2 over F, respectively, then the elements $\alpha_i\beta_j$ for $i=1,2,\cdots,n$ and $j=1,2,\cdots,m$ span K_1K_2 over F.

Proof) Let $\{\alpha_1,\cdots,\alpha_n\}$ and $\{\beta_1,\cdots,\beta_m\}$ be F-basis of K_1 and K_2 respectively. From lemma 16, we have $K_1K_2 = F(\alpha_1,\cdots,\alpha_n,\beta_1,\cdots,\beta_m)$. Then the element of K_1K_2 has the form

$$\sum_{1\le j\le m}\Big(\sum_{1\le i\le n} a_{ij}\alpha_i\Big)\beta_j \text{ with } a_{ij}\in F.$$ Thus, $\{\alpha_i\beta_j\}$ spans K_1K_2 over F and since $|\{\alpha_i\beta_j\}|\le n\cdot m$

KOKUYO LOOSE-LEAF J-836BT 6mm ruled, B5 size

prime : $(n,m)=1$. Then $[K_1K_2:F] = [K_1:F]\cdot[K_2:F] = n\cdot m$.

Proof) Since $[K_1K_2:F] = \ell$ is divisable n and m, $(\ell)\subset(n)$ and $(\ell)\subset(m)$ hold.

Thus, we have $(\ell)\subset(n)\cap(m)$. Since $(n)+(m)=(n,m)=R$, coprime, by Chinese remainder theorem, we have $(n)\cdot(m)=(n)\cap(m)$ and we have $(n)\cdot(m)=(n\cdot m)$.

Therefore, $(\ell)\subset(nm)$, nm divides ℓ. And by prop 21 we have $\ell\le nm$, so $\ell=nm$.

Prop 33. A polynomial $f(x)$ has a multiple root α iff α is also a root of $D_x f(x)$, i.e., $f(x)$ and $D_x f(x)$ are both divisible by the minimal polynomial for α. In particular, $f(x)$ is separable iff it is relatively prime to its derivative: $(f(x), D_x f(x)) = 1$

Proof) First we assert the first assertion.

($\Rightarrow$) Let α be a multiple root of $f(x)$. Then, $f(x) = (x-\alpha)^n g(x)$ for some $g(x) \in F[x]$, $n \in \mathbb{N}_{>1}$. Then, we have $D_x f(x) = n \cdot (x-\alpha)^{n-1} g(x) + (x-\alpha)^n D_x g(x)$, since $D_x f(\alpha) = 0$, α is a root of $D_x f(x)$.

($\Leftarrow$) By assumption, there exists $h(x) \in F[x]$ such that $f(x) = (x-\alpha) \cdot h(x)$ and since we have $D_x f(\alpha) = 0$. By $D_x f(x) = h(x) + (x-\alpha) \cdot D_x h(x)$ we obtain α is a root of $h(x)$, there exists $h'(x) \in F[x]$ such that $h(x) = (x-\alpha) \cdot h'(x)$. So, $f(x) = (x-\alpha)^2 \cdot h'(x)$. This show that α is a multiple root of $f(x)$.

To verify the particular case, it is enough to show that $f(x)$ has a multiple root iff $(f(x), D_x f(x)) \neq F$. This drived by the first assertion.

Cor 34. Every irreducible polynomial over a field of characteristic 0 is separable. A polynomial over such a field is separable iff it is the product of distinct irreducible polynomials.

Proof). First, we show the first assertion. Let F be a field with $\mathrm{ch}(F) = 0$ and let $f(x) \in F[x]$ be irreducible polynomial with degree n and assume that $n \geq 2$.

Now, since $D_x f(x) = (a_n \cdot n)\, x^{n-1} + \cdots = a_n (1 + \cdots + 1) \cdot x^{n-1} + \cdots$ and $\mathrm{ch}(F) = 0$, we have $\deg(D_x f(x)) = n-1$.

No.

Date

Since, $f(x)$ is irreducible, $p(x)$ cannot have $D_x f(x)$ as a factor. Thus, $(f(x), D_x f(x)) = 1$. By prop 33, $f(x)$ is separable.

Now we show the second assertion.

($\Rightarrow$) Since $f(x)$ has the form $a(x-a_1)\cdot\cdots\cdot(x-a_n)$, each $(x-a_i)$ is irreducible and distinct.

($\Leftarrow$) Let $f(x) = p_1(x)\cdot\cdots\cdot p_n(x)$ be a product of distinct irreducible polynomials. By first assertion, since every $p_i(x)$ is separable and irreducible, $\deg(p_i(x)) = 1$ must hold. Thus, $f(x)$ is separable.

Prop35. Let F be a field of characteristic p. Then for any $a, b \in F$, $(a+b)^p = a^p + b^p$, and $(a\cdot b)^p = a^p \cdot b^p$. Put another way, the pth-power map defined by $\varphi(a) = a^p$ is an injective field homomorphism from F to F.

Proof) $(a\cdot b)^p = a^p \cdot b^p$ is manifestly.

By the binomial theorem, we have $(a+b)^p = a^p + b^p + \sum_{1 \le i \le p-1} \binom{p}{i} a^{p-i} b^i$. Since $\binom{p}{i} = \frac{p!}{(p-i)!\,i!}$ and both of $(p-i)!$ and $i!$ does not have p as a factor, we have $p \mid \binom{p}{i}$ for every i. This assert $\binom{p}{i} a^{p-i} \cdot b^i = 0$ for every i since $\mathrm{ch}(F)$. Therefore, $(a+b)^p = a^p + b^p$.

Cor 36 Suppose that F is a finite field of characteristic p. Then every element of F is a p-th power of F.

Proof) An injective endomorphism on finite set is surjective. So, since F is finite the Frobenius endomorphism is surjection.

Prop1. $Aut(K)$ is a group under composition and $Aut(K/F_1)$ is a subgroup.

Proof) Clearly, $Aut(K)$ is a group. Let $\tau, \sigma \in Aut(K/F_1)$ and $x \in F_1$ then $(\tau \circ \sigma^{-1})(x) = \tau(\sigma^{-1}(x)) = \tau(x) = x$. Thus, $\tau \circ \sigma^{-1} \in Aut(K/F_1)$, $Aut(K/F_1)$ is a subgroup.

Prop2. Let K/F_1 be a field extension and let $\alpha \in K$ be algebraic over F_1. Then for any $\sigma \in Aut(K/F_1)$, $\sigma\alpha$ is a root of the minimal polynomial for α over F_1 i.e. $Aut(K/F_1)$ permutes the roots of irreducible polynomials. Equivalently, any polynomial with coefficients in F_1 having α as a root also has $\sigma\alpha$ as a root.

Proof) First, we show the first assertion. Let $\sum_{0 \le i \le n} a_i \cdot x^i$ be the minimal polynomial for α over F_1. Then by applying σ, we obtain $\sum_{0 \le i \le n} \sigma(a_i) \cdot (\sigma(\alpha))^i = 0$ and since $\sigma(a_i) = a_i$ for every i. Thus, $\sigma(\alpha)$ is a root of the minimal polynomial.

Since, for $f(x) \in F_1[x]$ with $f(\alpha)$ there exists $g(x) \in F_1[x]$ such that $f(x) = g(x) \cdot m_{\alpha, F_1}(x)$ then the second assertion is clearly.

Prop3 Let $H \le Aut(K)$ be a subgroup of the group of automorphism K. Then the collection F_1 of elements of K fixed by all the elements of H is a subfield of K.

Proof). Let $a, b \in F_1$, we show $a-b$, $a \cdot b^{-1} \in F_1$. For arbitrary $h \in H$, $h(a-b) = h(a) - h(b) = a - b$ and $h(a \cdot b^{-1}) = h(a) \cdot h(b)^{-1} = a \cdot b^{-1}$. Thus, F_1 is a subfield of K.

Prop4 The association of the groups to fields and fields of groups defined above is inclusion

KOKUYO LOOSE-LEAF A-SCIENT

reversing, namely

(1) if $F_1 \subseteq F_2 \subseteq K$ are two subfields of K then $Aut(K/F_2) \leq Aut(K/F_1)$, and

(2) if $H_1 \leq H_2 \leq Aut(K)$ are two subgroups of automorphisms with associated fixed fields F_1 and F_2, respectively, then $F_2 \subseteq F_1$.

Proof) (1) Let $\sigma \in Aut(K/F_2)$, since σ fixs evevery element in F_2, so is in F_1. Thus, $Aut(K/F_2) \leq Aut(K/F_1)$

(2) Let $a \in F_2$. Then for all $h \in H_2$, moreover for all $h \in H_1$, $h(a) = a$. Hence, $F_2 \subseteq F_1$.

Prop 5 Let E be the spliting field over F of the polynomial $f(x) \in F[x]$. Then $|Aut(E/F)| \leq [E:F]$ with equality if $f(x)$ is separable over F.

Proof). Note that for a field isomorphism $\varphi : F \to F'$ and polynomials $f(x) \in F[x]$ and $f'(x) \in F'[x]$, where $f'(x)$ is associated with $f(x)$ and φ and let E and E' be spliting fields for $f(x)$ over F and for $f'(x)$ over F', respectively. Then thm 13.19 assert there exists extented isomorphism $\sigma : E \to E'$.

Now, if the following assertion is true, the given assertion is clear.

The number of such an extension is at most $[E:F]$, with equality if $f(x)$ is separable over F.

We proved by induction on $[E:F]$.

If $[E:F]=1$, $E=F$ and $E'=F'$ thus $\varphi=\sigma'$, the number of extensions is 1.

Assume that $[E:F]\geq 2$.

By the proof of thm 13.17 if all the degree of irreducible factor of $f(x)$ is 1 then we have $E=F$. Let $p(x)$ be a irreducible factor of $f(x)$ with $\deg p(x)\geq 2$ and lets $p'(x)$ be a irreducible polynomial associated with φ and $p(x)$.

Lets α be a root of $p(x)$ and lets $\tau_\alpha : \sigma|_{F(\alpha)}$ and let $p(x)=\sum_{0\leq i\leq n} a_i\cdot x^i$, $a_n\neq 0$.

Since, we have $0=\tau_\alpha\left(\sum_{0\leq i\leq n} a_i\cdot\alpha^i\right)=\sum_{0\leq i\leq n}\tau_\alpha(a_i)\cdot(\tau_\alpha(\alpha))^i=\sum_{0\leq i\leq n}\varphi(a_i)\cdot(\tau_\alpha(\alpha))^i$, $\tau_\alpha(\alpha)$ is a root of $p'(x)$.

Now, by thm 13.8 we have an isomorphism $\tau_\alpha : F(\alpha)\approx F'(\beta)$ where $\beta=\tau_\alpha(\alpha)$.

Thus the number of extensions φ to τ_α is equals to the number of roots in $p(x)$. Since $\deg(p(x))=\deg(m_{\alpha,F}(x))=[F(\alpha):F]$. The number of extensions of φ is at most $[F(\alpha):F]$, with equality, if $p(x)$ is separable.

As we have seen in thm 13.27 E and E' are the spliting fields of $f(x)$ over $F(\alpha)$ and of $f'(x)$ over $F'(\beta)$, respectively, and $[E:F(\alpha)]<[E:F]$.

By the induction hypothesis, the number of extensions τ_α to σ is less than or equals to $[E:F(\alpha)]$, with equality if $f(x)$ is separable in $F(\alpha)[x]$.

Therefore, the number of extensions φ to σ is less than or equals to $[E:F(\alpha)]\cdot[F(\alpha):F]=[E:F]$ with equality if both of $f(x)$ and $p(x)$ are separable, $f(x)$ is separable in $F[x]$.

KOKUYO LOOSE-LEAF

Cor 6. If K is the spliting field over F of a separable polynomial $f(x)$ then K/F is Galois.

Proof). By thm 5, manifestly Galois.

Thm 7. If $\chi_1, \cdots, \chi_n$ are distinct characters of G with values in L then they are linearly independent over L.

Proof) We proved by induction on n. Since $n=1$ is clearly, assume that $n \geq 2$.

Suppose that $\sum_{1 \leq i \leq n} a_i \chi_i = 0$ for $a_i \in L$. Since $\chi_1 \neq \chi_n$ there exists $g_0 \in G$ we have $\chi_1(g_0) \neq \chi_n(g_0)$.

Now, for arbitrary $g \in G$ and g_0 we have the following equations

$$\left(\sum_{1 \leq i \leq n} a_i \cdot \chi_i(g)\right)\chi_n(g_0) = 0 \ , \ \sum_{1 \leq i \leq n} a_i \cdot \chi_i(g \cdot g_0) = 0$$

moreover, we have $\sum_{1 \leq i \leq n-1} \left(a_i (\chi_i(g_0) - \chi_n(g_0))\right) \chi_i(g) = 0$ for all g.

thus, $\sum_{1 \leq i \leq n-1} a_i \left(\chi_i(g_0) - \chi_n(g_0)\right) = 0$.

By induction hypothesis, $a_i \left(\chi_i(g_0) - \chi_n(g_0)\right) = 0$ for all $1 \leq i \leq n-1$, in paticular, we have $a_1 \left(\chi_1(g_0) - \chi_n(g_0)\right) = 0$ thus $a_1 = 0$ and by induction hypothesis we have $a_i = 0$ for all $1 \leq i \leq n$.

Cor 8 If $\sigma_1, \cdots, \sigma_n$ are distinct embeddings of a field K into a field L, then they are linearly independent as function on K. In paticular distinct automorphism of the extensions over their fixed fields.

Proof). By thm 7 clearly holds.

Thm 9 Let $G = \{\sigma_1 = 1, \sigma_2, \cdots, \sigma_n\}$ be a subgroup of automorphisms of a field K and let F be the fixed field. Then $[K : F] = n = |G|$.

Proof). First, we suppose that $n > [K:F] = m$. Let $\{w_1, \cdots, w_m\}$ be a basis of K/F. Then since $n > m$, for the equations,

$$\sum_{1 \le i \le n} \sigma_i(w_j)\, x_i = 0 \quad \cdots \quad (*_j) \quad \text{for all } 1 \le j \le m$$

there exists nontrivial solution $\beta_1, \cdots, \beta_n$ in K.

For $\alpha \in K$, there exists $a_1, \cdots, a_m \in F$ such that $\alpha = \sum_{1 \le i \le m} a_i \cdot w_i$. Now since σ_i fix F, by multiplying $(*_j)$ by a_j,

$$\sum_{1 \le i \le n} \sigma_i(a_j \cdot w_j) \cdot \beta_i = 0 \quad \cdots \quad (**_j) \quad \text{for all } 1 \le j \le m.$$

Moreover, $\sum_{1 \le j \le m} \sum_{1 \le i \le n} \sigma_i(a_j \cdot w_j)\, \beta_i = 0$, $\sum_{1 \le i \le n} \sigma_i(\alpha)\, \beta_i = 0$. Then Cor 8 assert every $\beta_i = 0$, a contradiction.

Next, we suppose that $n < [K:F]$. Let $\alpha_1, \cdots, \alpha_{n+1}$ be an $n+1$ F-linearly independent elements of K. Then since $n < n+1$, for the equations,

$$\sum_{1 \le i \le n+1} \sigma_j(\alpha_i) \cdot x_i = 0 \quad \cdots \quad (*_j) \quad \text{for } 1 \le j \le n$$

there exists nontrivial solutions $\beta_1, \cdots, \beta_{n+1}$ in K.

Now, suppose every $\beta_i \in F$. Then since $\sigma_1 = id$, by $(*_1)$ we have $\sum_{1 \le i \le n+1} \alpha_i\, \beta_i = 0$ this contradicts $\{\alpha_1, \cdots, \alpha_{n+1}\}$ is linearly independent. Thus $\beta_i \notin F$ for some i.

Now, we repicking $\beta_1, \cdots, \beta_{n+1}$ and reordering $\alpha_1, \cdots, \alpha_{n+1}$ such that r is the smallest number such that $\beta_i = 0$ iff $i > r$ and $\beta_1 \notin F$ and assume that $\beta_r = 1$.

Since, $\beta_1 \notin F$ there exists $\sigma_{k_0} \in G$ such that $\sigma_{k_0}(\beta_1) \neq \beta_1$.

KOKUYO KOSHIBAN ✓-RB8ST Unprinted 036 Brass

Then applying $(*_i)$ by σ_{k_0}, we have $\sum_{1\le i\le r} \sigma_{k_0}\sigma_j(\alpha_i)\,\sigma_{k_0}(\beta_i) = 0$ for $1\le j\le n$.

Since, for every j there exists k_j such that $\sigma_{k_0}\sigma_j = \sigma_{k_j}$. Thus we have the followings,

$$\sum_{1\le i\le r} \sigma_{k_0}(\beta_i)\,\sigma_{k_j}(\alpha_i) = 0 \quad \cdots\cdots \quad (**_j) \quad \text{for } 1\le j\le n.$$

Substracting $(**_j)$ by $(*_{k_j})$ we have $\sum_{1\le i\le r} \sigma_{k_j}(\alpha_i)\,(\sigma_{k_0}(\beta_i) - \beta_i) = 0$ for $1\le j \le n$. Since $\beta_r = 1$, $\sigma_{k_0}(\beta_1)-\beta_1, \cdots, \sigma_{k_0}(\beta_{r-1})-\beta_{r-1}, 0, \cdots, 0$ is the nontrivial solution for $(*)$ and this contradicts the picking of smallest r.

Therefore, we have $n\le m$ and $m\le n$. Hence $n = m$.

Cor10 Let K/F be any finite extension. Then $|\mathrm{Aut}(K/F)| \le [K:F]$ with equality if and only if F is the fixed field of $\mathrm{Aut}(K/F)$. Put another way, K/F is Galois if and only if F is the fixed field of $\mathrm{Aut}(K/F)$.

Proof) Let F_1 be the fixed field of $\mathrm{Aut}(K/F)$, then we have $F\subset F_1 \subset K$. By thm 9, we have $[K:F_1] = |\mathrm{Aut}(K/F)|$. Hence, $|\mathrm{Aut}(K/F)| \le [K:F_1]\cdot[F_1:F] = [K:F]$ with equality iff $[F_1:F] = 1$ i.e. F is the fixed field of $\mathrm{Aut}(K/F)$.

Cor11 Let G be a finite subgroup of automorphisms of a field K and let F be the fixed field. Then every automorphism of K fixing F is contained in G, i.e., $\mathrm{Aut}(K/F) = G$, so that K/F is Galois, with Galois group G.

Proof) By the definition of F, we have $G\le \mathrm{Aut}(K/F)$. Then by thm 9 and cor10, we obtain $[K:F] = G \le |\mathrm{Aut}(K/F)| \le [K:F]$. Thus, $|G| = |\mathrm{Aut}(K/F)|$, $G = \mathrm{Aut}(K/F)$ and since

we have $[K:F_1] = |\mathrm{Aut}(K/F_1)|$, K/F_1 is Galois.

Cor 12 If $G_1 \neq G_2$ are distinct finite subgroups of automorphism of a field K then their fixed fields are also distinct.

Proof.) Let F_1 and F_2 be the fixed fields associated with G_1 and G_2, respectively. Then by Cor11 we have, $G_1 = \mathrm{Aut}(K/F_1) = \mathrm{Aut}(K/F_2) = G$ if $F_1 = F_2$.

Prop 13 The extension K/F_1 is Galois iff K is the spliting field of some separable polynomial over F_1. Furthermore, if this is the case then every irreducible polynomial with coefficients in F_1 which has a root in K is separable and has all its roots in K.

Proof) ($\Leftarrow$) We already seen in prop 5.

($\Rightarrow$) At the beging of the proof we verify the "furthermae" part

Let K/F_1 be the Galois extension associated with irreducible polynomial $p(x) \in F_1[x]$ with root $\alpha \in K$. Let $G := \mathrm{Gal}(K/F_1) = \mathrm{Aut}(K/F_1)$ and for $G = \{id, \sigma_2, \cdots, \sigma_n\}$ consider a list $\alpha, \sigma_2(\alpha), \cdots, \sigma_n(\alpha)$ and let $\alpha_1, \cdots, \alpha_r$ be the distinct elements in this list.

Now, by applying the ordered list $\alpha_1, \cdots, \alpha_r$ by $\tau \in G$ is simply permutes the subscripts but the list without order. So, the polynomial $f(x) = (x-\alpha_1)\cdots(x-\alpha_r)$ is the polynomial which every coefficent is fixed by any element in G. Moreover, every coefficient of $f(x)$ is in fixed field of G and Cor10 assert since K/F_1 is Galois, its fixed field is F_1, hence $f(x)$ is the polynomial in $F[x]$. And since $f(x)$ has a roots α and $p(x)$ is the minimal polynomial, up to multipling an unit, we have $p(x) \mid f(x)$. Thus by prop 2, each α_i is a root of $p(x)$ so $f(x) \mid p(x)$ in

KOKUYO LOOSE-LEAF ASSORT

$K[x]$. Therefore, $f(x)$ is equals to $p(x)$, up to multiplying an unit. Now we compete the proof of "furthermore" part.

Next, we compere the proof of ($\Rightarrow$).

Let K/F be Galois and $\{w_1, \cdots, w_n\}$ be a basis of K over F and $p_i(x) = m_{w_i, F}(x)$ for each i. By the above argument, each $p_i(x)$ is separable and has all its root in K. Let $g(x)$ be the segnare free pant of the products $p_1(x) \cdots p_n(x)$. Then the spliting field of the products $p_1(x) \cdots p_n(x)$ and $g(x)$ are the segme and equals K.

Therefore, K is the spliting field of separable polynomial $g(x)$ over F.

Thm 14. Fundemental Theorem of Galois Theory.

Let K/F be a Galois extension and $G = Gal(K/F)$. Then there is a bijection

$$\left\{ \begin{array}{l} K \\ | \\ E \\ | \\ F \end{array} \right. \quad \text{subfields } E \text{ of } K \text{ containing } F \quad \left. \right\} \longleftrightarrow \left\{ \begin{array}{l} 1 \\ \\ H \\ \\ G \end{array} \right. \quad \text{subgroups of } G \left. \right\}$$

given by the correspondences $E \mapsto \{$the elements of G fixing $E\}$, $H \mapsto \{$the fixed field of $H\}$ which are inverse to each other. Under this correspondence,

(1) (inclusion reversing) If E_1, E_2 correspond to H_1, H_2, respectively, then $E_1 \subseteq E_2$ iff $H_2 \subseteq H_1$

(2) $[K:E] = |H|$ and $[E:F] = |G:H|$, the index of H in G:

$$\begin{array}{l} K \\ | \\ E \\ | \\ F \end{array} \quad \begin{array}{l} \} |H| \\ \\ \} |G:H| \end{array}$$

(3) K/E is always Galois, with Galois group $Gal(K/E) = H$:

K
$|$ H
E

(4) E is Galois over F iff H is a normal subgroup in G. If this is the case, then the Galois group is isomorphic to the quotient group $Gal(E/F) \simeq G/H$. More generally, even if H is not necessarily normal in G, the isomorphisms of E into a fixed algebraic closure of F containg K which fix F are in one to one correspondence with the cosets $\{\sigma H\}$ of H in G.

(5) If E_1, E_2 correspond H_1, H_2, respectively, then the intersection $E_1 \cap E_2$ corresponds to the group $\langle H_1, H_2 \rangle$ generated by H_1 and H_2 and the composite field E_1E_2 corresponds to the intersection $H_1 \cap H_2$. Hence the lattice of subfields of K containing F and the lattice of subgroups to G are "dual" (the lattice diagram for one is the lattice diagram for the other turned upside down.

Proof) At the begining of the proof, we verify the bijection corresponding. For $H \leq G$, Let K_H be the fixed field of H. Define $f : \{H ; 1 \leq H \leq G\} \to \{E ; F \leq E \leq K\} ; H \mapsto K_H$. By cor 12 f is injective. Let $f(x)$ be a separable polynomial which induce the spliting field K over F. Then we can consider K as the spliting field of $f(x)$ over F for every E, i.e., K/E is Galois. Thus by Cor 10, E is the fixed field of $Aut(K/E)$ which is the subgroup of G. Hence, f is surjective.

(1) Immediately by prop 4.

(2) For a given H, let $E = K_H$. Then by thm 9, $[K : E] = |H|$ since K/F is Galois, $|K : F| = |G|$

and by finiteness we have $[E:F] = \frac{[K:F]}{[K:E]} = \frac{|G|}{|H|}$.

(3) Directly derived from Cor 11.

(4) At the begining of the proof, we make some preparations. Let $E := K_H$ be the fixed field of $H (\leq G)$.

First, we assert every embedding τ of E fixing F has the form $\sigma|_E$ for some $\sigma \in G$.

Let $\tau : E \hookrightarrow \bar{F}$ be any embedding of E into a fixed algebraic closure $\bar{F}$ of F containing K which fixes F. Since, E is also algebraic over F, every $\alpha \in E$ has the minimal polynomial $m_{\alpha,F}(x)$ and by prop 2 $\tau(\alpha)$ is a root of $m_{\alpha,F}(x)$. So by thm 13, K contains all the roots of $m_{\alpha,F}(x)$, so $\tau(\alpha) \in K$, $\tau(E) \subseteq K$.

Let $f(x)$ be a separable polynomial which induce the spliting field K over F and $\tau(f(x))$ is also a separable polynomial which induce the spliting field K for every $\tau \in G$. Thus by thm 12.2.7 there exists isomorphism σ with $\sigma|_E = \tau$ as

$$\begin{array}{ccc} \sigma & : & K \sim K \\ & & | \quad | \\ \tau & : & E \sim \tau(E) \end{array}$$

Second, we assert E/F is Galois iff $\sigma(E) = E$ for all $\sigma \in G$.

For $\sigma, \sigma' \in G$, (3) assert that $\sigma|_E = \sigma'|_E$ iff $H\sigma = H\sigma'$ where $H\sigma$ and $H\sigma'$ are fixed field correspond to σ and σ', respectively. Then for $Emb(E/F) = \{\sigma : E \hookrightarrow \bar{F};\ fix\ F\}\ (\supseteq Aut(E/F))$, the number of distinct embeddings of E equals the number of cosets σH of H in G, so we obtain

$$|Emb(E/F)| = |G:H| \overset{(2)}{=} [E:F]$$

Thus, E/F is Galois iff $|Aut(E/F)| = |Emb(E/F)|$ iff $Aut(E/F) \supseteq Emb(E/F)$.

Moreover, we assert $Aut(E/F_1) \supseteq Emb(E/F_1)$ iff $\sigma(E) = E$ for all σ.

($\Rightarrow$) Let $\sigma \in G$, $\alpha \in E$. Since $\sigma|_E \in Emb(E/F_1) \subseteq Aut(E/F_1)$ we have $\sigma|_E(\alpha) \in E$.

($\Leftarrow$) Let $\sigma \in Emb(E/F_1)$. Since $\sigma(E) = E$ we have $\sigma \in Aut(E/F_1)$.

Now we prove (4)

($\Rightarrow$) Suppose E/F_1 is Galois, i.e., $\forall \sigma \in G$ $\sigma(E) = E$. Let $h \in H$ and $g \in G$ then clearly $ghg^{-1} \in Aut(K/F_1)$ and for $\alpha \in E$ there exists $\beta \in E$ such that $g(\beta) = \alpha$. Then since h fix E, $ghg^{-1}(\alpha) = \alpha \in E$ thus, $ghg^{-1} \in H$, i.e., $H \trianglelefteq G$.

($\Leftarrow$) $E := K_H$, $\sigma \in G$ and $\alpha \in E$ and by assumption for all $h \in H$, there exists $h' \in H$ such that $\sigma h' \sigma^{-1} = h$. Thus, we have $h\sigma(\alpha) = \sigma h^{-1}(\alpha) = \sigma(\alpha)$, $\sigma(E) \subset E$. Thus, E/F_1 is Galois.

Next, we show $G/H \approx Gal(E/F_1)$. Define a map $\varphi : G \to Gal(E/F_1) ; \sigma \mapsto \sigma|_E$. The well-definedness is because $\sigma|_E \in Aut(E/F_1)$ and we have $\ker \varphi = \{\sigma ; \varphi(\sigma) = \sigma|_E = id\} = Aut(K/E) = H$. Thus, we obtain $G/H \approx Gal(E/F_1)$.

And, by mimic the above poreses, we have the "more generally" part.

(5) $E_1 \cdot E_2 \longleftrightarrow H_1 \cap H_2$

It suffice to show that $H_1 \cap H_2 = Aut(K/E_1 E_2)$.

($\subseteq$) Let $\sigma \in H_1 \cap H_2$. Since σ fix E_1 and E_2 so does $E_1 \cdot E_2$.

($\supseteq$) Let $\sigma \in Aut(K/E_1 E_2)$. Since we have $E_1, E_2 \subseteq E_1 E_2$, $\sigma \in Aut(K/E_1)$, $Aut(K/E_2)$.

$E_1 \cap E_2 \longleftrightarrow \langle H_1, H_2 \rangle$

KOKUYO LOOSE-LEAF A-4SBT 6 mm ruled 26 lines

It suffice to show that $E_1 \cap E_2 = K^{\langle H_1, H_2 \rangle}$.

($\subseteq$) Let $\alpha \in E_1 \cap E_2$. For $\sigma \in \langle H_1, H_2 \rangle$ $\exists h_i \in H_1 \cup H_2$ with $\varepsilon_i \in \{\pm 1\}$ $\sigma = h_1^{\varepsilon_1} \cdots h_n^{\varepsilon_n}$. And every h_i fix α so does σ.

($\supseteq$) Let $\alpha \in K^{\langle H_1, H_2 \rangle}$. Since $H_1, H_2 \leq \langle H_1, H_2 \rangle$ so $\alpha \in E_1, E_2$ so we have $\alpha \in E_1 \cap E_2$.

Prop15 Any finite field is isomorphic to F_{p^n} for some prime p and some integer $n \geq 1$. The field F_{p^n} is the spliting field over F_p of the polynomial $x^{p^n} - x$, with cyclic Galois group of order n generated by the Frobenius automorphism σ_p. The subfields of F_{p^n} are all Galois over F_p and are in one to one correspondence with the divisors d of n. They are the fields F_{p^d}, the fixed fields of σ_p^d.

Proof) The first assertion drived by Cor 13.36. Now, we verify the first assertion. First, we show if the dimension is n, $[F, F_p] = n$, then F is a spliting field of $x^{p^n} - x$ over F_p.

Note that the number of elements in F is p^n and by Cor 13.37 $x^{p^n} - x$ has precisely p^n roots. For any roots α and β, by prop 13.35, we have $(\alpha\beta)^{p^n} = \alpha\beta$, $(\alpha^{-1})^{p^n} = \alpha^{-1}$ and $(\alpha+\beta)^{p^n} = \alpha+\beta$

Hence the spliting field of $x^{p^n} - x$ over F is a subfield of F_{p^n} however, since the cardinality of F and the same, F is the spliting field. Furthermore, by thm 13. (F_{p^n} / F_p) is a Galois, we have $\mathrm{Gal}(F_{p^n}/F_p) = \langle \sigma_p \rangle \simeq \mathbb{Z}/p\mathbb{Z}$ where $\sigma_p : F_{p^n} \to F_{p^n}$; $a \mapsto a^p$.

Now, we verify the last assertion. By the Fundemental Theorem of Galois Theory, every subfield of F_{p^n} corresponds, bijectively, to a subgroup of $\langle \sigma_p \rangle$ ($= \mathbb{Z}/p\mathbb{Z}$) and every subgroup of $\langle \sigma_p \rangle$ has the from $\langle \sigma_p^d \rangle$ where $d \mid n$. Let $F_{p^n}^{\langle \sigma_p^d \rangle}$ be the subfield which correspond to $\langle \sigma_p^d \rangle$.

By (2) in Fundemental Theorem of Galois Theory, we have $[F_{p^n} < \sigma_p^d > : F_p] = |< \sigma_p > : < \sigma_p^d >|$ $= \frac{n}{(\frac{n}{d})} = d$ and since $|F_p| = p$, we obtain $|F_{p^n} < \sigma_p^d >| = p^d$. Thus, by uniqueness of finite field, we have $F_{p^n} < \sigma_p^d > \approx F_{p^d}$. Therefore, every subfield of F_{p^n} has the form F_{p^d} which is isomorphic to fixed field $< \sigma_p^d >$ for some $d | n$.

At last, since $< \sigma_p >$ is an Abelian, every $< \sigma_p^d >$ is normal in $< \sigma_p >$ then by (4) in Fundemental theorem, every F_{p^d} is Galois over F_p.

Cor 16. The irreducible polynomial $x^4+1 \in \mathbb{Z}[x]$ is reducible modulo every prime p.

Proof). Note that by prop 9.11, x^4+1 is irreducible $\mathbb{Z}[x]$. We prove that x^4+1 is reducible in $F_p[x]$ for every prime p.

If $p=2$. Since, $(x+1)^4 = (x^2+1)^2 = x^4+1$, x^4+1 is reducible in $F_2[x]$.

If $p \neq 2$. Since for every odd number p, $p \equiv 1, 3, 5$ or $7 \pmod 8$ moreover, $p^2 \equiv 1 \pmod 8$, we have $p^2-1 = 8k$ for some k. Since, $x^{p^2-1} - 1 = x^{8k} - 1 = (x^8-1) \cdot p(x)$, $x^8-1 \mid x^{p^2-1} - 1$ in $F_p[x]$. This shows that every root of x^4+1 is a root of $x^{p^2} - x$ and the spliting field of $x^{p^2} - x$ over F_p is F_{p^2}, so every roots of x^4+1 contains in F_{p^2}.

Now, assume that x^4+1 is irreducible in $F_p[x]$ and let $\alpha \in F_{p^2}$ be any root of x^4+1. Then $x^4+1 = m_{\alpha, F_p(\alpha)}$, hence, $[F_p(\alpha) : F_p] = \deg(m_{\alpha, F(\alpha)}) = \deg(x^4+1) = 4$. On the other hand we have $[F_{p^2} : F_p] = 2$.

This contradicts, $[F_{p^2} : F_p] = [F_{p^2} : F_p(\alpha)] \cdot [F_p(\alpha) : F_p]$. Thus, x^4+1 is reducible in $F_p[x]$.

Prop. 17. The finite field F_{p^n} is simple. In paticular, there exists an irreducible polynomial of degree n over F_p for every $n \geq 1$.

Proof) First, we show the first assertion. Prop 9.18 assert that the finite multiplicative group $F_{p^n}^{\times}$ is a cyclic group, i.e., $F_{p^n}^{\times} = \langle \theta \rangle$ for some $\theta \in F_{p^n}^{\times}$ and the thm 15 assert F_{p^n} is the spliting field of $x^{p^n} - x$ over F_p, now, we verify the equation $F_{p^n} = F_p(\theta)$ holds.

"$\supseteq$" is clear. We check the conversely. Let $\alpha \in F_{p^n}$ and assume that $\alpha \neq 0$. Since, $\alpha \in F_{p^n}^{\times} = \langle \theta \rangle$. For some k, $0 \leq k \leq p^n - 2$, $\alpha = \theta^k$. Thus, $\alpha \in \{ \sum \alpha_i \cdot \theta^i \} = F_p(\theta)$, furthermore, $F_{p^n} = F_p(\theta)$.

Next, we verify the "in paticular". Since, for every $n \geq 1$, prop 13.11 assert $\deg(m_{\theta, F_p}(x)) = [F_p(\theta) : F_p] = [F_{p^n} : F_p] = n$, thus we pick $m_{\theta, F_p}(x)$ as desired irreducible polynomial.

Prop 19. Suppose K/F is a Galois extension and F'/F is any extension. Then KF'/F' is a Galois extension, with Galois group $Gal(KF'/F') \simeq Gal(K/K\cap F')$ isomorphic to a subgroup of $Gal(K/F)$.

Proof) Let K be the spliting field of separable polynomial $f(x) \in F[x]$ over F. Since $F \subseteq F'$ and KF' is the smallest field containing F' and K, we have $KF' = F'(\alpha_1, \cdots, \alpha_n)$ where α_i is a root of $f(x)$ so KF'/F' is Galois.

Next, we verify the group isomorphism. Define a map $\varphi : Gal(KF'/F') \to Gal(K/F)$; $\sigma \mapsto \sigma|_K$. This is clearly well-defined and since $\varphi(\sigma\circ\tau) = (\sigma\circ\tau)|_K = \varphi(\sigma)\circ\varphi(\tau)$, φ is a group homomaphism. And since $\sigma \in Aut(KF')$ fix F' and K so does KF' hence we obtain $\ker\varphi = id$, so φ is injective.

Now, we show $H := im\,\varphi = Gal(K/K\cap F')$. Let K_H be the fixed field of H. For every $\sigma \in Aut(KF'/F')$, since $\sigma|_K \in K_H$, σ fixes K_H and also fixes F' so does $K_H \cdot F$.

Thus, by Foundemental Theorem of Galois Theory, we have $K_H F' = K F'_{Gal(KF'/F)} = F'$ so, $K_H \subseteq F'$ moreover, $K_H \subseteq K \cap F'$.

Hence, by (1) in Foundemetal Theorem of Galois Theory, $H \geq Gal(K/K\cap F')$.

Therefore, $Gal(KF'/F) \simeq Gal(K/K\cap F')$.

Cor 20. Suppose K/F is a Galois extension and F'/F is any finite extension. Then

$$[KF' : F] = \frac{[K:F]\cdot[F':F]}{[K\cap F' : F]}.$$

Proof). By prop. 19 we have $[KF':F'] = [K : K \cap F']$. Thus,

$$[KF':F] = [KF':F'] \cdot [F':F] = [K : K \cap F'] \cdot [F' : F] = \frac{[K : K \cap F'] \cdot [K \cap F' : F]}{[K \cap F' : F]} [F' : F]$$

$$= \frac{[K : F]}{[K \cap F' : F]} [F' : F]$$

Prop 21. Let K_1 and K_2 be Galois extensions of a field F. Then

(1) The intersection $K_1 \cap K_2$ is Galois over F.

(2) The composite $K_1 K_2$ is Galois over F. The Galois group is isomorphic to the subgroup

$$H = \{ (\sigma, \tau) \; ; \; \sigma|_{K_1 \cap K_2} = \tau|_{K_1 \cap K_2} \}$$

of the direct product $Gal(K_1/F) \times Gal(K_2/F)$ consisting of elements whose restrictions to the intersection $K_1 \cap K_2$ are equal.

Proof) (1) For fixed $\alpha \in K_1 \cap K_2$. Since $K_1 \cap K_2 / F$ is finite, so is algebraic, consider $p(x) = m_{\alpha, F}(x)$. Since $\alpha \in K_1$ and K/F is Galois, by thm 13, $p(x)$ is separable and has all roots in K_1, similarly, $p(x)$ has all roots in K_2. Thus all the roots in $K_1 \cap K_2$. This shows that $K_1 \cap K_2$ is the spliting field of $p(x)$ over F.

(2) Let K_1 and K_2 be the spliting fields of separable polynomial $f_1(x)$ and $f_2(x)$ in $F[x]$, respectively. By thm 13.21, the composite $K_1 K_2$ is the spliting field of square part of $f_1(x) f_2(x)$. Thus, $K_1 K_2$ is Galois.

Next, we show the group isomorphism. Let $\varphi : Aut(K_1 K_2 / F) \to Aut(K_1/F) \times Aut(K_2/F) \; ; \; \sigma \mapsto (\sigma|_{K_1}, \sigma|_{K_2})$, this is clearly injective group homomorphism.

Now, we verify $H = im\,\varphi$. Since $im\,\varphi \subset H$ and H is finite, we show that the cardinality of H and $im\,\varphi$ are the same.

Note that for every $\sigma \in Gal(K_1/F)$, since for arbitrary $\tau \in Gal(K_2/F)$ with $\sigma|_{K_1 \cap K_2} = \tau|_{K_1 \cap K_2}$ there exists unique $\rho \in Gal(K_2/K_1 \cap K_2)$ such that $\tau = \rho \circ \sigma|_{K_1 \cap K_2}$, there are $|Gal(K_2/K_1 \cap K_2)|$ elements $\tau \in Gal(K_1/K_1 \cap K_2)$ such that $\sigma|_{K_1 \cap K_2} = \tau|_{K_1 \cap K_2}$ and by third isomorphism theorem and cor 20, we obtain

$$\begin{aligned} |H| &= |Gal(K_1/F_1)| \cdot |Gal(K_2/K_1 \cap K_2)| \\ &= |Gal(K_1/F_1)| \cdot \frac{|Gal(K_2/F_1)|}{|Gal((K_1 \cap K_2)/F_1)|} \\ &= \frac{[K_1 : F_1] \cdot [K_2 : F_1]}{[K_1 \cap K_2 : F_1]} \\ &= [K_1 \cdot K_2 : F_1]. \end{aligned}$$

Cor 22. Let K_1 and K_2 be Galois extensions of a field F_1 with $K_1 \cap K_2 = F_1$. Then $Gal(K_1 \cdot K_2/F_1) \cong Gal(K_1/F_1) \times Gal(K_2/F_1)$. Conversely, if K is Galois over F_1 and $G = Gal(K/F_1) = G_1 \times G_2$ is the distinct product of two subgroups G_1 and G_2, then K is the composite of two Galois extensions K_1 and K_2 of F_1 with $K_1 \cap K_2 = F_1$.

Proof) The first assertion derived by prop 21. We verify the secound assertion. Let K_1, K_2 be the fixed fields associated with G_1, G_2, respectively. Since $G = G_1 \times G_2$, we have $\langle G_1, G_2 \rangle = G$. By (5) in Foundemental Theorem of Galois Theorem, we obtain $K_1 K_2$ corresponds to $G_1 \cap G_2 = id$. Therefore, $K_1 \cdot K_2 = K_{id} = K$ and also by (5), $K_1 \cap K_2$ corresponds to $\langle G_1, G_2 \rangle = G$. Therefore, $K_1 \cap K_2 = K_G = K_{Gal(K/F)} = F_1$.

Cor 23. Let E/F be any finite separable extension. Then E is contained in an extension K which is Galois over F and is minimal in the same that in a fixed algebraic closure of K any other Galois extension of F containing E contains K.

Proof) Let $\{\alpha_1, \cdots, \alpha_n\}$ be a basis of E over F, let E_i be the spliting field of $m_{\alpha_i, F}(x)$.

Note that every $m_{\alpha_i, F}(x)$ is separable since E/F is separable extension. Thus, the composite field $E_1 E_2 \cdots E_n$ $(\supseteq E)$ is Galois over F since $E_1, \cdots, E_n$ is the spliting field of the squarefree part of $m_{\alpha_1}(x) \cdots m_{\alpha_n}(x)$. Thus, a Galois extensions of F containg E exists. Then, the intersection of its Galois extension is minimal Galois extension containing E.

Prop24. Let K/F be a finite extension. Then $K = F(\theta)$ iff there exists only finitely many subfields of K containing F.

Proof) $(\Rightarrow)$ Let $f(x) = m_{\theta, F}(x)$, E be a subfield of K containing F and let $g(x) = m_{\theta, E}(x)$. Since $F \subseteq E \subseteq K$ and K/F is finite extension, by minimality $g(x) \mid f(x)$ in $E(x)$.

Let $E' = F(a_{n-1}, \cdots, a_0)$ for $g = \sum_{0 \le i \le n} a_i x^i \in E[x]$. Since, $E' \subset E$, $g(x)$ is irreducible in E' and $g(x) = m_{\theta, E'}(x)$ and moreover, since $F \subset E \subset K$, we have $E(\theta) = K$ and $E'(\theta) = K$ so, we have $[K : E] = \deg g(x) = [K : E']$. Thus, we have $[E' : E] = 1$, so $E = E'$. This shows that the subfield of K containing F are the field generated by the coefficient of monic factors of $f(x)$. So the subfields are only finitely many.

$(\Leftarrow)$ Let $[K : F] = n$ with basis $\{k_1, \cdots, k_n\}$. If F is finite, $F \simeq \mathbb{F}_{p^m}$, since for every $\alpha \in K$ there exists n-triple $(a_1, \cdots, a_n) \in \mathbb{F}^n$ such that $\alpha = \sum_1 a_i k_i$, so the cardinality of K is $(p^m)^n$, $K \simeq \mathbb{F}_{p^{mn}}$.

By thm 17, $K/\mathbb{F}_p$ is simple, $K = \mathbb{F}_p(\theta)$ for some $\theta \in K$.

Now, we assert $K = F(\theta)$. $F(\theta) \subset K$ is clearly so we verify $K \subset F(\theta)$.

Let $\beta \in K$ then there exists $\beta_i \in F_p$ with $\beta = \sum_i \beta_i \theta^i$. Since $\beta_i \in F$ we obtain $\beta \in F(\theta)$. Hence $K = F(\theta)$.

Hereafter, we assume that F is infinite.

Thm 13.17 asserts that K is finitely generated over F, it suffice to shows that for every α and $\beta \in K$, $F(\alpha, \beta) = F(\gamma)$ for some γ.

Consider the subfield $F(\alpha + c\beta)$ for $c \in F$. Since there exists there exists infinitely many choice for c, then by assumption for some distinct c and c' in F, $F(\alpha + c\beta) = F(\alpha + c'\beta)$ holds.

Then by $(c - c')\beta = (\alpha + c\beta) - (\alpha + c'\beta) \in F(\alpha + c\beta)$ we have $\beta = (c - c')\beta \cdot (c - c')^{-1} \in F(\alpha + c\beta)$ and $\alpha = (\alpha + c\beta) - c\beta \in F(\alpha + c\beta)$. Hence, $F(\alpha, \beta) = F(\alpha + c\beta)$.

Thm 25. (The Primitive Elements Theorem)

If K/F is finite and separable, then K/F is simple. In paticular, any finite extension of fields of characteristic 0 is simple.

Proof) Let L be the Galois clouser of K over F. Then since L/F is Galois, every subfield of L containing F corresponds bijectively to the subgroup of $Gal(L/F)$. Thus, every subfield of K containing F corresponds injectively to the subgroup of $Gal(L/F)$. Now, since $|L : F|$ is finite, there exists only finitely many subgroups of $Gal(L/F)$. Thus by thm 24 K/F is simple.

Now, we show the "in paticular" part. For every $\alpha \in K$ and the minimal polynomial $m_{\alpha, F}(x)$, Cor 13.34 assert $m_{\alpha, F}(x)$ is separable. Hence K/F separable and by (1) we complete the proof.

Prop 30 The fixed field of the symmetric group S_n acting on the field of rational functions in n variables $F(x_1, \cdots, x_n)$ is the field of rational functions in the elementary symmetric functions $F(s_1, \cdots, s_n)$.

Proof) Let K be the fixed field of S_n. Then since every $\sigma_i \in S_n$ is symmetric, K contains $F(s_1, \cdots, s_n)$ and since $F(x_1, \cdots, x_n) = F(s_1, \cdots, s_n)(x_1, \cdots, x_n)$ is Galois, by Fundemental Theorem of Galois Theory, $[F(x_1, \cdots, x_n) : K] = |S_n| = n!$. Since we have $(x - x_1) \cdots (x - x_n) = \sum_{0 \le i \le n} (-1)^i s_i x^i$ with $s_0 = 1$, $F(x_1, \cdots, x_n)$ is the spliting field of $\sum_{0 \le i \le n} (-1)^i s_i x^i$ over $F(s_1, \cdots, s_n)$. Then by prop 13.26 $[F(x_1, \cdots, x_n) : F(s_1, \cdots, s_n)] \le n!$. Hence, we have $n! \cdot [K : F(s_1, \cdots, s_n)] \le n!$, $K \cong F(s_1, \cdots, s_n)$ Therefore, $K = F(s_1, \cdots, s_n)$.

Cor 31 Fundemental Theorem on Symmetic Functions.

Any symmetric function in the variables $x_1, \cdots, x_n$ is a rational function in the elementary symmetric functions $s_1, \cdots, s_n$.

Proof) Since every symmetric function is in the fixed field of S_n, so by prop 30 it contained in $F(s_1, \cdots, s_n)$.

Thm 32 The general polynomial $x^n - s_1 x^{n-1} + s_2 x^{n-2} + \cdots + (-1)^n s_n$ over the field $F(s_1, \cdots, s_n)$ is separable with Galois group S_n.

Proof) Let $x_1, \cdots, x_n$ be the roots of $x^n - s_1 x^{n-1} + \cdots + (-1)^n s_n$. If there exists a polynomial $p(t_1, \cdots, t_n) \in F[t_1, \cdots, t_n]$ such that $p(x_1, \cdots, x_n) = 0$, we define $\tilde{p}(t_1, \cdots, t_n) = \prod_{\sigma \in S_n} p(t_{\sigma(1)}, \cdots, t_{\sigma(n)})$ then $\tilde{p}$ is non-zero and $\tilde{p}(x_1, \cdots, x_n) = 0$. Since $\tilde{p}$ is symmetric, Cor 31 assert there exists a polynomial $\tilde{q}(u_1, \cdots, u_n) \in$

KOKUYO LOOSE-LEAF A-836BT 6 mm ruled × 30 lines

$F(u_1, \cdots, u_n)$ such that $\tilde{\varphi}(t_1, \cdots, t_n) = \tilde{f}(u_1, \cdots, u_n)$ where $u_1, \cdots, u_n$ are elementaly symmetric functions induced by $t_1, \cdots, t_n$ and note that $u_i(x_1, \cdots, x_n) = s_i$ for every i. Then we obtain an equation $\tilde{f}(u_1(x_1, \cdots, x_n), \cdots, u_n(x_1, \cdots x_n)) = \tilde{\varphi}(x_1, \cdots, x_n) = 0$. This assert there exists a relation over F among $s_1, \cdots, s_n$, a contradiction.

Therefore, there is no relation over F among $x_1, \cdots, x_n$, moreover, $x_i \neq x_j$ if $i \neq j$. Hence the given polynomial is reparable and prop30 and the Fundemental Theorem of Galois Theory assert the Galois group is S_n.

Prop 36. Let F be a field of characteristic not dividing n which contains the nth roots of unity. Then the extension $F(\sqrt[n]{a})$ for $a \in F$ is cyclic over F of degree dividing n.

Proof) First, we show that $F(\sqrt[n]{a})/F$ is Galois. Since the characteristic of F not divide n, we have $(x^n - a, D_x(x^n - a)) = (x^n - a, n \cdot x^{n-1}) = 1$. Then by prop 13.33, $x^n - a$ is separable in $F[x]$.

Now, we verify $K := F(\sqrt[n]{a})/F$ equals the spliting field S of $x^n - a$ over F, since $K \subset S$ is clearly, it suffice to show that the reverse inclusion. Recall that, by prop 9.18, $C = \{\alpha \in F ; \alpha^n = 1\}$ is cyclic group, so we may write $C = \langle \zeta_n \rangle$. Since, $C \subset F \subset K$ and $\sqrt[n]{a} \in K$ we have $\mu_n := \{\zeta_n^i \sqrt[n]{a} ; 1 \le i \le n\} \subseteq K$ and since $(\zeta_n^i \sqrt[n]{a})^n = a$ this means that K contains all the root of $x^n - a$ s.o. $S \subseteq K$. Therefore, K is the Galois extension of $x^n - a$ over F.

Next, we verify $Gal(K/F)$ is cyclic. For $\sigma \in Gal(K/F)$, $\sigma(\sqrt[n]{a})$ is a root of $x^n - a \in F[x]$ thus, for some i, we have $\sigma(\sqrt[n]{a}) = \zeta_n^i \cdot \sqrt[n]{a}$. In this case we construct a map $\varphi : Gal(K/F) \to C$ which assign the σ the suitable $\zeta_n^i \sqrt[n]{a}$. Since every $\sigma \in Gal(K/F)$ fixes C, φ is group homomorphism also, $\ker \varphi = \{\sigma \in Gal(K/F) ; \zeta_n^i \sqrt[n]{a} = \sqrt[n]{a}\} = \{\sigma \in Gal(K/F) ; \sigma(\sqrt[n]{a}) = \sqrt[n]{a}\} = \{id\}$.

Thus, we have $Gal(K/F) \approx \operatorname{im} \varphi \le C$. Therefore, since C is cyclic, so does $Gal(K/F)$ and moreover, Lagrange Theorem assert $|Gal(K/F)| \mid n$.

Prop 37. Any cyclic extension of degree n over a field F of characteristic not dividing n which contains the nth roots of unity is of the form $F(\sqrt[n]{a})$ for some $a \in F$.

Proof). Let K be a such extension and let $Gal(K/F) = \langle \sigma \rangle$ and $\mu_n = \langle \zeta \rangle = \{a \in F ; a^n = 1\}$

KOKUYO LOOSE-LEAF A-836DT 6 mm ruled 36 lines

In general, for $\alpha \in K$ and $\zeta \in F$ with $\zeta^n = 1$. Since, $\zeta^{n-1} = \zeta^{-1}$ and $\sigma^n = 1$ hold, we have,

$$\sigma((\alpha, \zeta)) = \sigma(\alpha) + \zeta\sigma^2(\alpha) + \cdots + \zeta^{n-1}\sigma^n(\alpha)$$

$$= \zeta^{-1}(\alpha + \cdots + \zeta^{n-2}\sigma^{n-2}(\alpha) + \zeta^{n-1}\sigma^{n-1}(\alpha))$$

$$= \zeta^{-1}(\alpha, \zeta).$$

Thus, $\sigma((\alpha, \zeta)^n) = (\sigma(\alpha, \zeta))^n = (\alpha, \zeta)^n$, so $(\alpha, \zeta)^n \in K\,\mathrm{Gal}(K/F) = F$.

Now, Cor 8 assert $\{id, \sigma, \cdots, \sigma^{n-1}\}$ are linearly independent over F. hence for some $\alpha \in K$, we have $\sigma^i(\alpha, \zeta) = \zeta^i(\alpha, \zeta)$, σ^i does not fix (α, ζ) for some i for fixed α with $(\alpha, \zeta) \neq 0$.

Hence, by Fundemental Theorem of Galois Theory, there are no subfield of K containing F and (α, ζ).

Therefore, since $(\alpha, \zeta) \in F(\alpha, \zeta)$, $K = F(\alpha, \zeta)$. Hence by setting $a = (\alpha, \zeta)^n \in F$ we have $K = F(\sqrt[n]{a})$.

Lemma 38 If α is contained in a root extension K as in (21) above, then α is contained in a root extension which is Galois over F and where each extension K_{i+1}/K_i is cyclic.

Proof). Since the characteristic of F is 0 and K/F is finite, Cor 13.19 assert K is separable extension. Then by Cor 23, let L be the Galois clouser of K over F.

For any $\sigma \in \mathrm{Gal}(K/F)$ we have

$$F = \sigma(K_0) \subseteq \sigma(K_1) \subseteq \cdots \subseteq \sigma(K_s) = \sigma(K)$$

and every $\sigma(K_{i+1}) / \sigma(K_i)$ is a simple radical extension, i.e., $\sigma(K_{i+1}) = \sigma(K_i)(\sigma(\sqrt[n_i]{a}))$.

Now, we show that the composite of two root extensions is also a root extension. Let $F = K_0 \subset K_1 \subset \cdots \subset K_k$ and $F = S_0 \subset S_1 \subset \cdots \subset S_s$ be root extensions with $K_{i+1} = K_i(a_i)$ and $S_{j+1} = S_j(b_j)$. Then we have a sequence

$$F = K_0(a_0) \subset K_0(a_0)(b_0) \subset K_0(a_0)(b_0)(a_1) \subset \cdots \subset K_0(a_0)(b_0)(a_1)\cdots(b_{s-1}).$$

Note that the equation $K_k \cdot S_s = K_0(a_0)(b_0)(a_1)\cdots(b_{s-1})$ derived from the equation $K_1 S_1 = K_0(a_0)(b_0)$.

Therefore, for $\{\sigma_1, \cdots, \sigma_n\} = Gal(K/F)$, we have the root extension $\sigma_1(K)\cdot\sigma_2(K)\cdot\cdots\cdot\sigma_n(K)$.

Next, we verify $L_1 = \sigma_1(K)\cdots\sigma_n(K)$. Since "$\supset$" is clear, and L_1 is the minimal Galois extension containing K, it suffice to show that $\sigma_1(K)\cdots\sigma_n(K)$ is Galois, moreover, as we seen in the proof of thm14(2), it is enough to show that $Emb(\sigma_1(K)\cdots\sigma_n(K)/F) \subset Aut(\sigma_1(K)\cdots\sigma_n(K)/F)$.

Let $\tau \in Emb(\sigma_1(K)\cdots\sigma_n(K)/F)$. Then for each i, $\tau\circ\sigma_i|_K \in Emb(L/F) = Aut(L/F)$ holds and τ is injective. We have $\{\tau\circ\sigma_1|_K, \cdots, \tau\circ\sigma_n|_K\} = \{\sigma_1, \cdots, \sigma_n\}$ and since every $\sigma_i(K), (\tau\sigma_i)(K)$ is finite extension, we have $\tau(\sigma_1(K)\cdots\sigma_n(K)) = (\tau\circ\sigma_1)(K)\cdots(\tau\circ\sigma_n)(K)$.

Hence, we have $\tau(\sigma_1(K)\cdots\sigma_n(K)) = \sigma_1(K)\cdots\sigma_n(K)$, so $\tau \in Aut(\sigma_1(K)\cdots\sigma_n(K)/F)$.

Therefore, $\alpha \in K \subseteq L_1 = \sigma_1(K)\cdots\sigma_n(K)$, so α contained in a root extension which is Galois over F.

Finally, we show that K_{i+1}/K_i is cyclic extension. We assert for a Galois root extension $F = K_0 \subset \cdots \subset K_s = K$ with $K_{i+1} = K_i(\sqrt[n_i]{a_i})$, there exists a Galois root extension $F = F_0 \subset \cdots \subset F_t = K$ with $Gal(F_{j+1}/F_j)$ is cyclic.

Let F' be the field obtained by adjoining to F all the n_i th roots of unity for all $n_i, 0 \le i \le s-1$, i.e.,

KOKUYO LOOSE-LEAF

$F_1' = F \cup \{ \cup \{ n_i \text{ th roots of unity} \}, 0 \le i \le s-1 \}$. Since, F_1' is the spliting field of the squarefree part of $\prod_{0 \le i \le s-1} (x^{n_i} - 1)$, so the extension F'/F is Galois, moreover, by prop 21, $K \cdot F'/F$ is Galois.

Thus, we have the following Galois root extension :

$$F \subset F' = F' K_0 \subseteq F' K_1 \subset \cdots \subset F' K_s = F' \cdot K \quad \cdots (*)$$

Note that for every i, since $F' \cdot K_{i+1} = (F' \cdot K_i)(\sqrt[n_i]{\bar{a}_i})$ and F' contains all the n_i th roots of unity, by prop 36, $F' K_{i+1} / F' K_i$ is a cyclic extension.

Let ζ_{n_i} be the primitive n_i th roots of unity for every $0 \le i \le s-1$ and defince $F_{i+1} = F_i(\zeta_{n_i})$, then we have the folowing root extension :

$$F = F_0 \subset F_1 \subset \cdots \subset F_s = F \quad \cdots (**)$$

Since, every F_{i+1} is the spliting field of $x^{n_i} - 1$ over F_i, as we seen in the proof of prop 36, every F_{i+1}/F_i is cyclic extension.

Therefore, by concatenate $(*)(**)$, we obtain the desired Galois root extension.

Thm 39 The polynomial $f(x)$ can be sloved by radicals iff its Galois group is a solvable group.

Proof) ($\Rightarrow$) Lemma 38 assert for each root d_i of $f(x)$ there exists a Galois root extension K_{d_i} with $d_i \in K_{d_i}$ and $K_{d_i i+1} / K_{d_i i}$ is cyclic. Let L_1 be the finitely many composition of $K_{d_1} \cdots K_{d_m}$. Then, as we seen the proof of lemma 38, L_1 is a Galois root extension and by construction of L_1 and Fundemental Theorem of Galois Theory, we have L_{i+1}/L_i is cyclic..

By Fundemental Theorem of Galois Theory, we have the following sequence of group.

$$Gal(L/F) = G_0 \geq G_1 \geq \cdots \geq G_s = id.$$

Thus, $Gal(L/F)$ is solvable.

Let K be the Galois extension of $f(x)$ over F, since $F \subset K \subset L$, by Fundamental Theorem of Galois Theory, we have $Gal(K/F) \approx Gal(L/F) / Gal(L/K)$ and by Third Isomorphism Theorem, $(G_{i+1} / Gal(L/K)) / (G_i / Gal(L/K)) \approx G_{i+1} / G_i$.

Therefore, by the following chain, $Gal(K/F)$ is solvable:

$$Gal(K/F) \approx Gal(L/F)/Gal(L/K) \geq G_1 / Gal(L/K) \geq \cdots \geq id.$$

($\Leftarrow$) Let K be the spliting field of $f(x)$ over F. Then we have the following chain:

$$id = G_s \trianglelefteq G_{s-1} \trianglelefteq \cdots \trianglelefteq G_1 \trianglelefteq G_0 = Gal(K/F)$$

with every G_i/G_{i+1} is a finite Abelian group.

Now, we assert for a normal subgroup $H \trianglelefteq G$, if G/H is finite Abelian group, there is a chain $H = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n \trianglelefteq H_{n+1} = G$ with H_{i+1}/H_i is cyclic.

Since, G/H is finite, G/H is a torsion $\mathbb{Z}$-module. Thus by thm 12.5 and thm 12.9, since $\mathbb{Z}$ is P.I.D., we have $G/H \approx \mathbb{Z}/(a_1) \oplus \cdots \oplus \mathbb{Z}/(a_m)$ with $(a_m) \subset \cdots \subset (a_1)$.

Since, $\mathbb{Z}/(a_1) \trianglelefteq G/H$, by the Fourth Isomorphism Theorem, there exists H_1 such that $H_0 \trianglelefteq H_1 \trianglelefteq G$ and $H_1/H_0 = \mathbb{Z}/(a_1)$. Moreover, by the Third Isomorphism Theorem, we obtain $G/H_1 \approx (G/H_0)/(H_1/H_0) \approx \mathbb{Z}/(a_2) \oplus \cdots \oplus \mathbb{Z}/(a_m)$. Again, there exists H_2 such that $H_1 \trianglelefteq H_2 \trianglelefteq G$ and $H_2/H_1 = \mathbb{Z}/(a_2)$ moreover, $G/H_2 \approx (G/H_1)/(H_2/H_1) \approx \mathbb{Z}/(a_3) \oplus \cdots \oplus \mathbb{Z}/(a_m)$.

KOKUYO LOOSE-LEAF ノ-ES6BT 6 mm ruled×36 lines

Continuing this process we have $H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_m \trianglelefteq G$ with H_{i+1}/H_i and G/H_m are cyclic.

Therefore, we obtain the chain,

$id = H_t' \trianglelefteq H_{t-1}' \trianglelefteq \cdots \trianglelefteq H_1' \trianglelefteq H_0' = Gal(K/F)$ with every H_i'/H_{i+1}' is cyclic.

Then, by the Fundamental Theorem of Galois Theory, we have the following chain:

$K = K_t \geq K_{t-1} \geq \cdots \geq K_1 \geq K_0 = F$ with every K_{i+1}/K_i is cyclic extension.

Let $n_i = [K_{i+1} : K_i]$ and define F' by adjoining to F all the n_i th roots of unity for every i.

Then we have the chain $F \subset F' = F' \cdot K_0 \leq F' K_1 \leq \cdots \leq F' \cdot K_t = F' \cdot K$ and since K_{i+1}/K_i is Galois and $F' \cdot K_i / K_i$ is extension, prop 19 shows that every $F' K_{i+1}/F' \cdot K_i$ is Galois and $Gal(F' \cdot K_{i+1}/F' \cdot K_i)$ $\approx Gal(K_{i+1}/K_{i+1} \cap F' \cdot K_i) \hookrightarrow Gal(K_{i+1}/K_i) \approx \mathbb{Z}/n_i\mathbb{Z}$. This shows that every $Gal(F' K_{i+1}/F' K_i)$ is cyclic and which order dividing n_i for every i, furthermore, every $F' K_{i+1}/F' K_i$ is cyclic.

Since, F' contains all the n_i th root of unity, moreover, every m which divide $n_i' := [F' K_{i+1}/F' K_i]$ divide n_i and the characteristic of $F'K$ is 0, by prop 37, we obtain $F' K_{i+1} = F' K_i (\sqrt[n_i]{a_i})$ for some $a_i \in F' \cdot K_i$. Moreover, we already seen in the proof of lemma 38, there exists a simple radical extension from F to F'. Therefore, KF' is a simple radical extension.

Since, $K \subseteq F' \cdot K$, each root of $f(x)$ is contained in $F' K$, $f(x)$ can be sloved by radicals.

Cor 40. The general equation of degree n cannot be sloved by radicals for $n \geq 5$.

Proof). Thm 32 assert the general polynomial is separable with Galois group S_n. If S_n is not a slovable group for $n \geq 5$, by thm 39, the general polynomial cannot be solved by radicals. Thus we

remain to show that S_n is not solvable for $n \geq 5$.

Let $n \geq 5$. Since the maximal proper subgroup of S_n is A_n and A_n is simple and is not normal in S_n. Thus, S_n does not possesses nontrivial subgroup, i.e., S_n is not solvable.