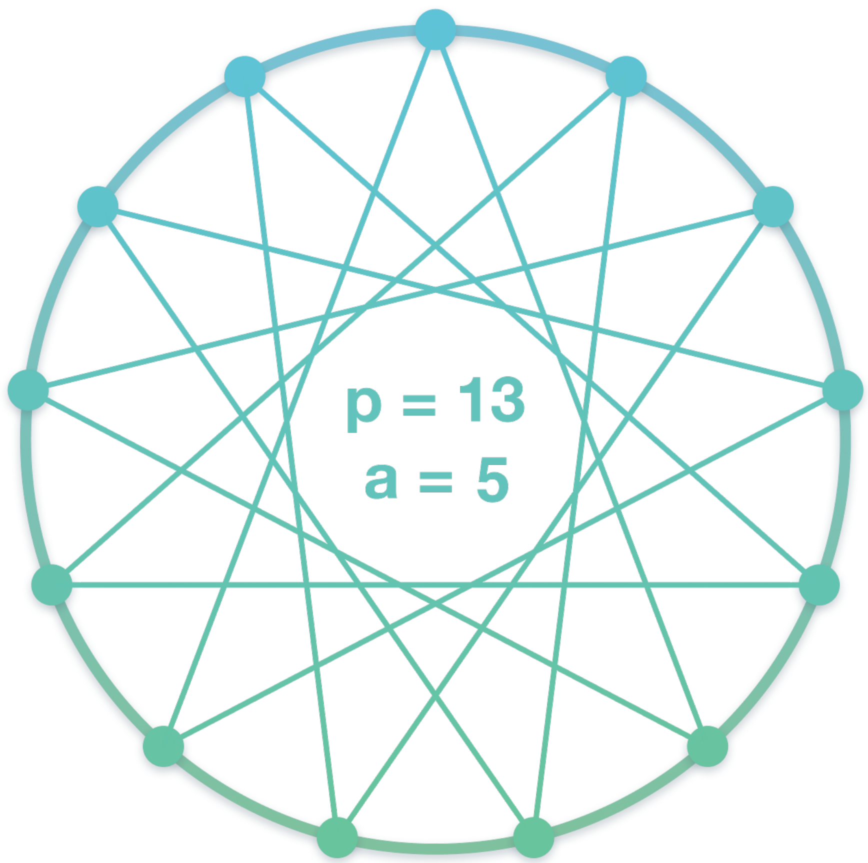
군론 복습노트

디멘(최정담)



1. 기초 개념

퍼뮤테이션

퍼뮤테이션의 분해. 유한집합의 퍼뮤테이션은 서로소인 순환cycle의 곱이다.

cf. 해당 순환들이 퍼뮤테이션의 **궤도orbit**

순환의 분해. 유한집합의 순환은 **전치transposition**의 곱이다. (pf. 삽입 정렬)

예)

- $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 4 & 3 & 1 \end{pmatrix} = (1, 6)(2, 5, 3)$
- $(2, 5, 3) = (2, 3)(2, 5)$

케일리의 정리. 모든 군은 어떤 순열군permutation group의 부분군이다.

퍼뮤테이션 분해의 기우성. 퍼뮤테이션 σ를 전치곱 $\tau_n \dots \tau_2\tau_1$으로 분해했을 때, n의 기우성은 σ에만 의존하다.

증명.

1. σ가 순열이고 τ가 전치일 때, $|\mathrm{Orb}(\sigma\tau)| = |\mathrm{Orb}(\sigma)| \pm 1$
2. 따라서 $\sigma = (\tau_n \dots \tau_2\tau_1)\iota$일 때 (ι는 항등원) n의 기우성은 |Orb(σ)|에 의해 결정됨.

따름정의. σ를 전치곱으로 분해했을 때 길이가 짝수(홀수)라면 σ를 짝(홀)순열이라고 한다.

따름정의. {1, …, n}의 짝순열로 이루어진 군을 **교대군 A_n**이라고 한다.

정리. n ≥ 5일 때 A_n은 단순군이다.

라그랑주 정리

보조정리: **잉여류의 단사성.** H ≤ G일 때, a ∈ G에 대하여 |H| = |aH| = |Ha|이다.

라그랑주 정리. 유한군 G의 부분군 H에 대해 |H| | |G| 이다.

따름정리: **라그랑주 위수 정리.** 유한군 G의 원소 a에 대해 Ord(a) | |G| 이다.

따름정리: **베주 정리.** $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n} \simeq \mathbb{Z}_{\mathrm{lcm}(m_1, \dots, m_n)}$

아벨군

유한생성아벨군의 기본정리. 유한생성아벨군은 다음의 꼴로 유일하게 분해된다. ($\{p_i\}$는 중복 포함 가능)

$$\mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_n^{r_n}} \times \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{\text{Betti number}}$$

따름정리: **아벨군에 대한 라그랑주 정리의 역.** 아벨군 G에 대해 $m \mid |G|$라면 G는 크기가 m인 부분군을 가진다.

따름정리: **아벨군에 대한 순환군 소수 판정법.** 아벨군 G에 대해 $p^2 \mid |G|$인 소수 p가 없다면 G는 순환군이다.

정의. $\{ [a, b] = aba^{-1}b^{-1} : a, b \in G \}$를 포함하는 G의 가장 작은 부분군을 **커뮤테이터 부분군** C(G)라고 한다.

아벨몫군 정리. G/H가 아벨군일 필요충분조건은 $C(G) \leq H$인 것이다.

정규부분군

정규부분군의 하급성. $H \leq K \leq G$일 때, $H \triangleleft G$라면 $H \triangleleft K$이다.

Note. $H \triangleleft K \triangleleft G$이지만 $H \triangleleft G$가 아닐 수 있다.

정리. $\phi: G \to G'$가 준동형 사상일 때,

1. $N \triangleleft G$라면 $\phi[N] \triangleleft \phi[G]$이다.
2. $M \triangleleft \phi[G]$라면 $\phi^{-1}[M] \triangleleft G$이다.

정리. $H_1 \triangleleft G_1$, $H_2 \triangleleft G_2$일 때 $H_1 \times H_2 \triangleleft G_1 \times G_2$이며, $(G_1 \times G_2)/(H_1 \times H_2) \cong (G_1/H_1) \times (G_2/H_2)$

순환군

순환군 소수 판정법. |G|가 소수라면 G는 순환군이다.

순환군의 생성자. 위수가 n인 순환군은 $\phi(n)$개의 생성자를 가진다.

Remark.

Additive → 베주 정리

Multiplicative → 페르마/오일러 정리

2. 준동형 사상

제1기본정리

단사성 판정법. 커널이 0인 준동형 사상은 단사함수이다.

준동형사상의 기본정리. $\phi: G \to G'$가 준동형 사상이고 $N \triangleleft G$이며 $\pi: G \to G/N$가 표준적 투영 사상일 때, 다음이 성립한다.

- $N \subset \ker \phi \quad \Rightarrow \quad \exists!\ \lambda: G/N \to G'$, λ는 전사
- $N = \ker \phi \quad \Leftrightarrow \quad \exists!\ \lambda: G/N \to G'$, λ는 동형

$$\begin{tikzcd} G \arrow[r, "\phi"] \arrow[d, "\pi"'] & G' \\ G/N \arrow[ur, dashed, "\exists!\lambda"'] & \end{tikzcd}$$

중심화군과 정규화군

정의. 군 G의 부분집합 S에 대해, $C_G(S) = \{ g \in G : gs = sg \quad \text{for all } s \in S\}$

정의. 군 G의 부분집합 S에 대해, $N_G(S) = \{ g \in G : gS = Sg \}$

정의. $Z(G) = \{ g \in G : gg' = g'g \quad \text{for all } g' \in G \}$

정리.

1. $Z(G) \triangleleft G$
2. G는 아벨군이다 $\quad \Leftrightarrow \quad Z(G) = G$
3. $Z(G) = \cap_{g \in G} C_G(g) = C_G(G)$
4. $H \leq G$일 때, $N_G(H)$는 H를 정규부분군으로 가지는 G의 가장 큰 부분군이다.

정리. $C_G(S) \triangleleft N_G(S) \leq G$

증명. $\phi: N_G(S) \to \mathrm{Bij}(S); g \mapsto (s \mapsto gsg^{-1})$에 대해 $\ker \phi = C_G(S)$

N/C 정리. G의 부분군 H에 대해 $N_G(H)/C_G(H)$는 $\mathrm{Aut}(H)$의 부분군과 동형이다.

증명. $\phi: N_G(H) \to \mathrm{Aut}(H); g \mapsto (h \mapsto ghg^{-1})$에 대해 $C_G(S) \subset \ker \phi$이므로 $\exists\lambda: N_G(H)/C_G(H) \to \mathrm{Aut}(H)$

제2기본정리

정의. $H, K \le G$일 때 $H \vee K$를 $HK = \{hk : h \in H, k \in K\}$를 포함하는 가장 작은 군으로 정의한다.

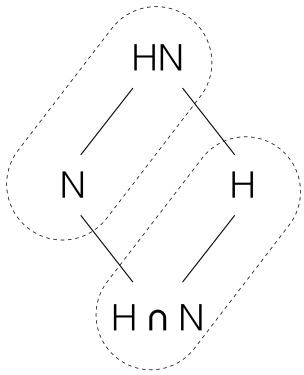
Note. 일반적으로 HK는 군이 아니다.

정리.

1. $N \lhd G$, $H \le G$일 때 $N \vee H = NH = HN \le G$이다.
2. $N \lhd G$, $M \lhd G$일 때 $NM \lhd G$이다.

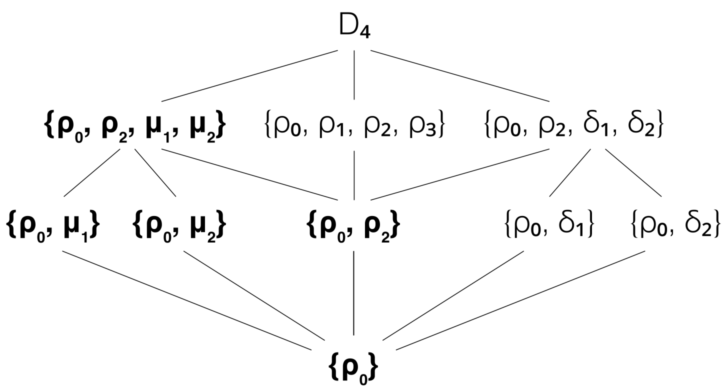
제2기본정리. $H \le G$이고 $N \lhd G$일 때 다음이 성립한다.

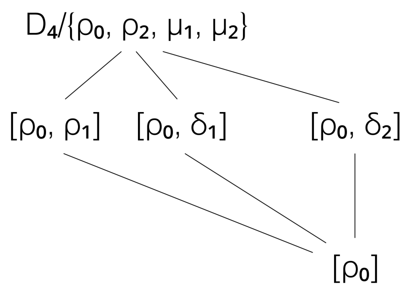
- $HN \le G$
- $N \lhd HN$
- $H \cap N \lhd H$
- $(HN)/N \cong H/(H \cap N)$



격자 정리

정리. $N \lhd G$이고 $\pi: G \to G/N$가 표준적 투영 사상일 때, π는 N을 포함하는 G의 모든 부분군과, G/N의 모든 부분군을 일대일 대응한다.





3. 군의 작용

군의 작용

정의. 군 G와 집합 X에 대해 * : G × X → X가 다음 조건들을 만족할 때 *는 X에 대한 G의 **작용**이다.

1. ex =x
2. $\forall g_1, g_2 \in G$ $g_2(g_1x) = (g_2g_1)x$

Note. * : G × X → X는 g를 Aut(X)로 대응시키는 함수, 즉 *: G → (X → X)로 이해할 수 있음 (cf. 람다 대수)

번사이드 정리

정의. Gx = { gx : g ∈ G }를 x의 **궤도**라고 한다.

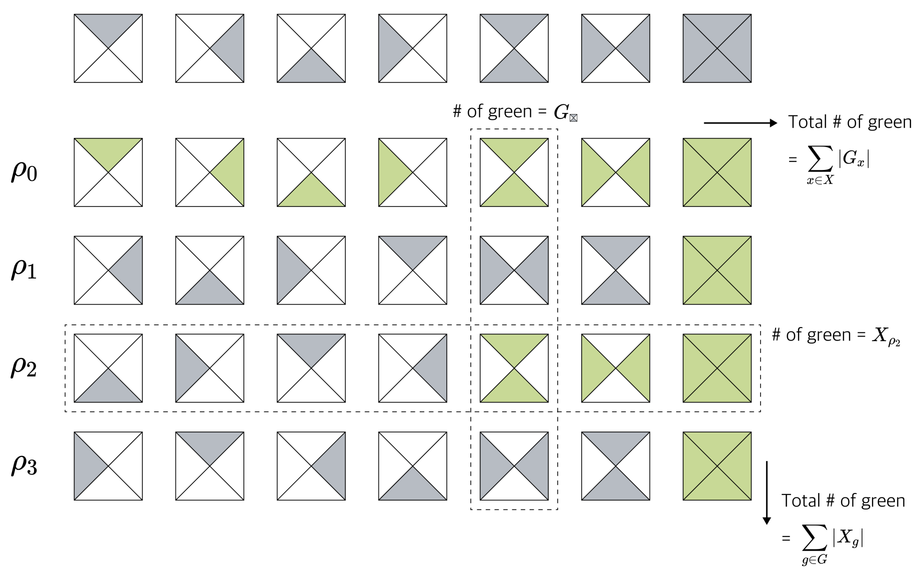
정의. G_x = { g ∈ G : gx = x }를 x의 **안정자군**이라고 한다.

정의. X_g = { x ∈ X : gx = x }를 **g-고정자**라고 한다.

궤도-안정자군 정리. $|G_x|\ |Gx| = |G|$

번사이드 정리. (# of orbits) = $(\Sigma_{g \in G} X_g) / |G|$

증명. (# of orbits) = $\Sigma_{x \in X}$ (1 / |Gx|) = $\Sigma_{x \in X}$ ($|G_x|$ / |G|) = $(\Sigma_{g \in G} X_g)$ / |G|



4. 군열

군열

정의.

1. $H_0 = \{e\} \triangleleft H_1 \triangleleft \dots \triangleleft H_n = G$인 군열 $\{H_0, \dots, H_n\}$을 **준정규군열**이라고 한다.
2. $H_0 = \{e\} \triangleleft H_1 \triangleleft \dots \triangleleft H_n = G$이고 $H_i \triangleleft G$인 군열 $\{H_0, \dots, H_n\}$을 **정규군열**이라고 한다.

Note.

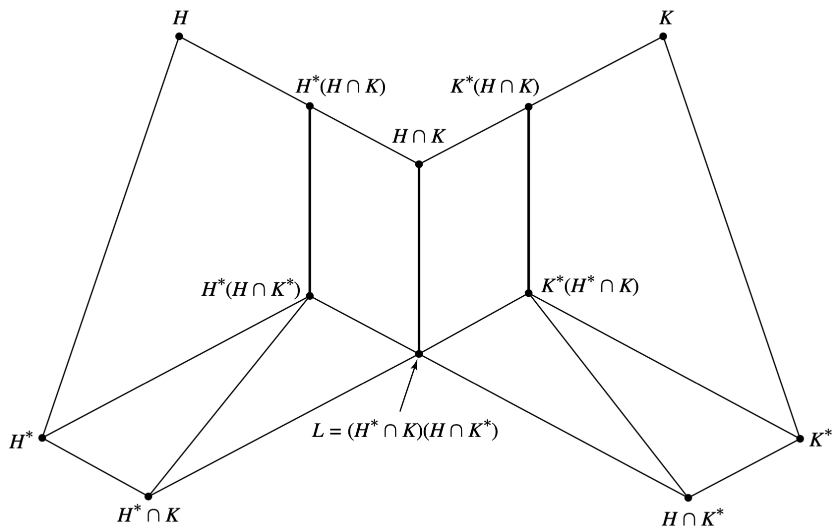
i. 정규군열에서 $H_0 \triangleleft H_1 \triangleleft \dots \triangleleft H_n$ 대신 $H_0 \leq H_1 \leq \dots \leq H_n$만 확인해도 충분.

ii. G가 아벨군일 때 준정규군열 ⇔ 정규군열

슈라이어 정리

차센하우스 보조정리 (나비 정리). $H, K \leq G$이고 $H^* \triangleleft H$, $K^* \triangleleft K$일 때, 다음이 성립한다.

1. $H^*(H \cap K^*) \triangleleft H^*(H \cap K)$
2. $K^*(H^* \cap K) \triangleleft K^*(H \cap K)$
3. $(H^*(H \cap K)) / (H^*(H \cap K^*)) \cong (K^*(H \cap K)) / (K^*(H^* \cap K))$



정의. G의 두 (준)정규군열 $\{H_i\}_{i\in I}$와 $\{K_j\}_{j\in J}$가 동형이라는 것은 $H_{i+1} / H_i \cong K_{j+1} / K_j$가 되도록 하는 일대일 대응 $\phi: I \to J$가 존재한다는 것이다.

슈라이어 정리. G의 임의의 두 (준)정규군열은 동형인 세분을 가진다. 즉, $\forall\{H_i\}, \{K_j\}\ \ \exists\{H_i\} \subset \{H_i'\}, \{K_j\} \subset \{K_j'\}$ s.t. $\{H_i'\} \cong \{K_j'\}$.

증명. 각 i에 대해 다음 군열을 고려하자.

$$H_i \le H_i(H_{i+1} \cap K_0) \le H_i(H_{i+1} \cap K_1) \le \dots \le H_i(H_{i+1} \cap K_m) = H_{i+1}$$

$$K_j \le K_j(K_{j+1} \cap H_0) \le K_j(K_{j+1} \cap H_1) \le \dots \le K_j(K_{j+1} \cap H_n) = K_{j+1}$$

차센하우스 정리에 의해 위 두 식에서 $\le$는 $\triangleleft$이고,

$$\Sigma_{ij} := H_i(H_{i+1} \cap K_{j+1})/H_i(H_{i+1} \cap K_j) \cong K_j(K_{j+1} \cap H_{i+1})/K_j(K_{j+1} \cap H_i)$$

이다.

<u>예시</u>. 다음의 두 군열이 주어졌을 때,

$$\{0\} \triangleleft 8\mathbb{Z} \triangleleft 4\mathbb{Z} \triangleleft \mathbb{Z}$$

$$\{0\} \triangleleft 9\mathbb{Z} \triangleleft \mathbb{Z}$$

다음과 같이 세분하면 동형이다.

$$\{0\} \triangleleft 72\mathbb{Z} \triangleleft 8\mathbb{Z} \triangleleft 4\mathbb{Z} \triangleleft \mathbb{Z} \qquad (\mathbb{Z}_{72} - \mathbb{Z}_9 - \mathbb{Z}_2 - \mathbb{Z}_4)$$

$$\{0\} \triangleleft 72\mathbb{Z} \triangleleft 18\mathbb{Z} \triangleleft 9\mathbb{Z} \triangleleft \mathbb{Z} \qquad (\mathbb{Z}_{72} - \mathbb{Z}_4 - \mathbb{Z}_2 - \mathbb{Z}_9)$$

정의. G의 준정규군열 $\{H_i\}$에서 각 i에 대해 H_{i+1}/H_i가 단순군이라면, $\{H_i\}$는 구성열이다.

조르당-횔더 정리. G의 임의의 두 구성열은 동형이다.

증명. 슈라이어 정리의 따름정리

정의. G의 구성열 $\{H_i\}$에서 각 i에 대해 H_{i+1}/H_i가 아벨군이라면 G는 **가해군**이다.

정리. A_5는 비가해군이다.

5. 실로우 정리

실로우 정리

정의. G의 모든 원소의 위수가 p일 때 G를 **p-군**이라고 한다.

정의. G가 X에 작용할 때, $X_G = \{ x \in X : \forall g \in G \;\; gx = x \}$를 **고정자**라고 한다.

고정자 모듈로-p 정리. G가 p-군이고 G가 X에 작용할 때, $|X| \equiv |X_G| \pmod p$

증명. $|X| = |X_G| + \Sigma_{O \in Orb(X), |O| \neq 1} |O|$. $|O| \neq 1$일 때 궤도-안정자군 정리에 의해 $p \mid |O|$.

정규화군 모듈로-p 정리. H가 G의 p-부분군일 때 $(N(H) : H) \equiv (G : H) \mod p$

증명. $X = G/H$로 두고 작용 $* : H \times X \to X; h \mapsto (gH \mapsto (hg)H)$으로 정의하여 고정자 모듈로-p 정리를 적용

코시의 정리. $p \mid |G| \Rightarrow$ G는 크기가 p인 부분군을 가진다.

증명.

1. $X = \{ (g_1, \ldots, g_p) : g_1 \ldots g_p = e \}$를 정의 $\to |X| = |G|^{p-1}$.
2. $\sigma = (1, 2, \ldots, p)$인 순환을 고려. $<\sigma>$는 크기가 p.
3. <u>고정자 모듈로-p 정리</u>에 의해 $|X| \equiv |X_{<\sigma>}| \equiv 0 \pmod p$. $(e, \ldots, e) \in X_{<\sigma>}$이므로 $p \mid |X_{<\sigma>}|$
4. $\therefore \exists g \neq e \in G : g^p = 1 \to \{e, g, g^2, \ldots, g^p\}$는 크기가 p인 G의 부분군

따름정리. G는 p-군이다 $\Leftrightarrow |G| = p^n$

실로우 정리. G가 크기 $p^n m$인 군일 때 (p와 m은 서로소) 다음이 성립한다.

1. 각 $1 \leq i \leq n$에 대하여 G는 크기 p^i인 부분군을 가진다.

   <u>따름정의</u>. G의 크기 p^n인 부분군을 **실로우-p 부분군**이라고 한다.
2. G의 p^i-부분군은 어떤 p^{i+1}-부분군의 정규부분군이다.
3. G의 서로 다른 두 실로우-p 부분군 P_1과 P_2은 공액conjugate 관계에 있다.
4. G의 실로우-p 부분군들의 개수 n_p는 <u>$n_p \mod p = 1$</u>과 <u>$n_p \mid m$</u>을 만족한다.

증명.

1. 코시의 정리와 수학적 귀납법을 적용.
   i. H가 크기 p^i $(i < m)$인 부분군이라고 하자. 정규화군 모듈로-p 정리에 의해 $(N(H) : H) \equiv (G : H) \equiv 0 \mod p \to p \mid N(H)/H$.
   ii. 코시의 정리에 의해 $\exists K \leq N(H)/H : |K| = p$. 표준 사영 사상 $\pi: N(H) \to N(H)/H$에 대해 $\pi^{-1}(K)$는 크기 p^{i+1}인 G의 부분군.
2. 1의 (ii)에서 $H < \pi^{-1}(K) \leq N(H)$. $H \triangleleft N(H)$이므로 $H \triangleleft \pi^{-1}(K)$.
3. 고정자 모듈로-p 정리를 사용.
   i. $*: P_1 \to (G/P_2 \to G/P_2); p \mapsto (gP_2 \mapsto pgP_2)$를 고려.
   ii. 고정자 모듈로-p 정리에 의해 $| (G/P_2)_{P_1} | \equiv |G/P_2| \neq 0 \mod p$.
   iii. 따라서 $\exists g \in G : \forall p \in P_1\ p(gP_2) = gP_2$이며, 해당 g에 대해 $gP_2g^{-1} = P_1$
4.
   i. G의 실로우-p 부분군 P를 모든 실로우-p 군들의 집합 ß에 가하는 conjugation 작용으로 생각하자. 만약 $S \in ß_P$라면 $\forall p \in P: pSp^{-1} = S$이므로 $S, P \leq N[S]$이다. 즉, S, P는 N[S]의 실로우-p군이므로 제2 실로우 정리에 의해 $\exists n \in N[S]: nSn^{-1} = P$이다. 따라서 $S = P$이며 $|ß_P| = 1$이다. 이제 고정자 모듈로-p 정리에 의해 $|ß| = |n_p| \equiv |ß_p| = 1 \mod p$를 얻는다.
   ii. G를 ß에 가하는 conjugation 작용으로 생각하고 궤도-안정자군 정리를 적용하면 $(G : G_P) = |G \cdot P| = n_p$이다. 여기서 $G_P = N[P]$이며, $P \leq N[P] \leq G$이므로 $|G| = p^n m$일 때 $|N[P]| = p^n k\ (k \mid m)$이다. 따라서 $m/k = n_p \Rightarrow n_p \mid m$.

실로우 정리의 응용

정리. 다음이 성립한다.

- 크기가 p^n인 군은 가해군이다.
- 크키가 p^2인 군은 아벨군이다.
- 크기가 pq인 군은 단순군이 아니다. (p, q는 서로 다른 소수)

정리. $H, K \leq G$일 때, $|HK| = (|H| \cdot |K|) / |H \cap K|$

따름정리. 크기가 $p^r (r > 1)$인 군은 단순군이 아니다.

6. 자유군

자유아벨군

정리. G가 아벨군이고 $X = \{x_1, \ldots, x_r\}$가 G의 부분집합이라고 하자. TFAE:

1. $\forall g \in G\ \exists! n_1, \ldots, n_r: g = n_1x_1 + \ldots + n_rx_r$
2. $G = \langle X \rangle \wedge (n_1x_1 + \ldots + n_rx_r = 0 \Rightarrow n_1 = \ldots = n_r = 0)$
3. $G \cong \mathbb{Z}^r$

따름정의. G가 위의 세 조건을 만족할 때 G를 자유아벨군이라고 하며, X를 G의 기저라고 한다.

정리. G가 유한한 기저를 가지는 자유아벨군이라면, G의 기저는 모두 유한하며 크기가 같다.

증명. X가 크기 r의 G-기저일 때, $G/2G \cong (\mathbb{Z}/2\mathbb{Z})^r$이므로 $\log_2 |G/2G| = r$.

따름정의. X가 G의 기저일 때 |X|를 G의 랭크라고 한다.

유한생성아벨군의 기본정리

보조정리.

1. G가 랭크 n인 자유아벨군일 때, G의 부분군 H는 랭크 $m \leq n$의 자유아벨군이다.
2. 어떤 G의 기저 $Y = \{x_1, \ldots, x_n\}$가 존재하여 $X = \{d_1x_1, \ldots, d_mx_m\}$가 H의 기저이고, $d_i \mid d_{i+1}$이다.

증명.

1. G의 기저 B에 대해, $m_0(B) = \min_{h \in H}$ [$h = k_1y_1 + \ldots + k_ny_n$에서 0을 제외한 가장 작은 계수]를 정의.
2. G의 모든 기저에 대해, m(B)가 최소인 기저 $Y_0 = \{y_1, \ldots, y_n\}$을 선택하자.
    1. Y_0의 정의에 의해 어떤 $w \in H$가 존재하여 WLOG $w = d_1y_1 + k_2y_2 + \ldots + k_ny_n$이고 d_1은 G의 기저 전개가 가질 수 있는 최소 계수이다.
    2. 나눗셈 알고리즘으로 $w = d_1(y_1 + q_2y_2 + \ldots q_ny_n) + r_2y_2 + \ldots r_ny_n$로 적을 수 있다. 그런데 $r_i < d_1$이고 d_1은 최소 계수이므로 $r_i = 0$이다.
    3. 따라서 $x_1 := y_1 + q_2y_2 + \ldots q_ny_n$일 때 $Y_1 = \{x_1, y_2, \ldots, y_n\}$ 또한 G의 기저이며, $d_1x_1 = w \in H$이다.

3. x_1을 포함하는 G의 기저 B에 대해, $m_1(B) = \min_{h \in H}$ [$h = k_1x_1 + k_2y_2 + \dots + k_ny_n$에서 k_1과 0을 제외한 가장 작은 계수]를 정의.
   1. 2와 같은 논리에 의해 기저 $Y_2 = \{x_1, x_2, y_3, \dots, y_n\}$가 존재하여 $d_1x_1, d_2x_2 \in K$이다.
   2. $d_1x_1 + d_2x_2 = d_1(x_1 + qx_2) + rx_2 \in K$이며, $r < d_1$이므로 $r = 0$. $\therefore d_1 \mid d_2$
   3. 이상의 논리를 귀납적으로 반복.

정리. 모든 유한생성아벨군은 다음의 꼴로 표현되며, $d_i \mid d_{i+1}$이다.

$$\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_r} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$$

증명. G가 n개의 원소로 생성될 때, 랭크 n인 자유아벨군 F에 대해 표준적으로 정의된 $\phi: F \to G$를 고려. $G \cong F/\ker\phi$이고, $\ker\phi$는 F의 부분군이다. 보조정리를 적용하면 원하는 결과를 얻음.

자유군

정의. 알파벳 $A = \{a_1, \dots, a_n\}$에 대해, A로 생성되는 형식적 단어들의 집합에 형식적 곱이 연산으로 주어진 군 F[A] 및, F[A]와 자연스럽게 동형인 군들을 자유군이라고 한다.

정리.

1. 군 G가 A와 B 위에서 자유일 때, A와 B의 기수는 같다. ⇒ 따름정의: $|A|$를 G의 랭크로 정의.
2. 두 자유군이 동형일 필요충분조건은 랭크가 같은 것이다.
3. 자유군의 부분군은 자유군이다.

자유군의 보편 성질. G가 $A = \{a_i\}_{i \in I}$ 위에서의 자유군일 때, 임의의 군 G'과 G'의 부분집합 $\{b_i\}_{i \in I}$에 대해 $\phi(a_i) = b_i$를 만족하는 준동형 사상 $\phi: G \to G'$은 유일하게 존재한다.

따름정리. 임의의 군 G는 어떤 자유군 F의 부분군이다.

증명. 군 G와 같은 기수의 집합 A에 대해, 자유군 F = F[A]는 보편 성질에 의해 G로 가는 준동형 사상을 가짐.

자유군과 자유아벨군. F가 A로 생성되는 자유군일 때, F의 커뮤테이터 부분군 C에 대해 F/C는 A로 생성되는 자유아벨군이다.

7. 표현 이론

군의 표현

Motivation. 모든 군은 자유군의 부분군이므로, 준동형 사상의 기본정리에 의해 어떤 자유군의 몫군으로 생각할 수 있음 → $G \cong F[A]/N$일 때, A와 $\langle r \in N \rangle$로써 G를 표현

정의. 집합 A에 대해 $\{r_i\} \subset F[A]$라고 하자. 또한 R이 $\{r_i\}$를 포함하는 F[A]의 가장 작은 정규부분군이라고 하자.

- 준동형 사상 $\phi: F[A]/R \to G$를 G의 표현이라고 한다.
- $(A : \{r_i\})$를 군 표현이라고 한다.
- A는 표현의 생성자이다.
- 각각의 $r \in R$은 $\{r_i\}$의 귀결이다.
- 각각의 $r_i = 1$을 관계라고 한다.
- A와 $\{r_i\}$가 유한할 때 유한 표현이라고 한다.

예시.

- $G = (a : a^6 = 1)$은 크기 6의 순환군 $\mathbb{Z}_6$이다.
- $G = (a, b : a^2, b^3, aba^{-1}b^{-1})$은 $aba^{-1}b^{-1} = 1$에 의해 아벨군이다. 따라서 $G = \{a^r b^s\}(0 \leq r < 2, 0 \leq s < 3)$은 크기가 6이며, 유한생성아벨군의 기본정리에 의해 $\mathbb{Z}_6$이다.

일반적으로 주어진 군의 표현은 유일하지 않다. 동형인 군을 표현하는 두 표현을 동형 표현이라고 한다.

정리.

- 주어진 두 표현이 동형인지 판단하는 일반적인 알고리즘은 존재하지 않는다.
- 주어진 표현이 특정 단어를 생성하는지 판단하는 일반적인 알고리즘은 존재하지 않는다(word problem).
- 주어진 표현이 유한군/아벨군/자유군/자명군인지 판단하는 일반적인 알고리즘은 존재하지 않는다.

군의 분류

예시. 크기 10인 군 G의 분류 문제.

1. 유한생성아벨군의 기본정리에 의해 크기 10인 아벨군은 모두 $\mathbb{Z}_2 \times \mathbb{Z}_5 \cong \mathbb{Z}_{10}$.
2. 비아벨군을 분류하기 위해 실로우 정리를 사용.
   1. G는 실로우-5 부분군 H을 가짐 → $\exists b \in G - H$: $b^2 \in H$. H의 모든 원소는 1을 제외하고 위수 5이므로, $b^2 \neq 1$이라면 b의 위수는 10이 되어 G는 순환군이 됨. $\therefore b^2 = 1$.
   2. G는 실로우-2 부분군 K를 가짐 → 위와 같은 논리에 의해 $\exists a \in G - K$: $a^5 = 1$.
3. $A = \{a, b\}$로 이루어진 표현 중 비아벨군인 경우$(ab \neq ba)$는 다음 세 가지. (Note: $ba = a^i b$에 의해 G의 모든 원소는 $a^r b^s$ 꼴로 표현 가능하므로 각 표현이 생성하는 군의 크기는 최대 10)
   1. $(a, b: a^5 = 1, b^2 = 1, ba = a^2 b)$
      - $a = b^2 a = b(ba) = b(a^2 b) = (ba)(ab) = (a^2 b)(ab)= a^2(ba)b = a^2(a^2 b)b = a^4 b^2 = a^4$. 따라서 $a^3 = 1$이 되어 모순.
   2. $(a, b: a^5 = 1, b^2 = 1, ba = a^3 b)$
      - $a = b^2 a = b(ba) = b(a^3 b) = (ba)(a^2 b) = (a^3 b)(a^2 b)= a^3(ba)(ab) = a^3(a^3 b)(ab) = a^6(ba)b = a^6(a^3 b)b = a^9 = a^4$. 따라서 $a^3 = 1$이 되어 모순.
   3. $(a, b: a^5 = 1, b^2 = 1, ba = a^4 b)$
      1. 아이디어: $S = \{a^0b^0, a^1b^0, a^2b^0, a^3b^0, a^4b^0, a^0b^1, a^1b^1, a^2b^1, a^3b^1, a^4b^1\}$에 다음의 표준canonical 연산을 주어 군으로 만들기

$$(a^s b^t)(a^u b^v) = a^x b^y \quad \text{where} \quad \begin{aligned} x &= s + u(4^t) \mod 5 \\ y &= t + v \mod 2 \end{aligned}$$

      2. 위의 연산이 군을 정의할 필요충분조건(즉, 결합법칙을 만족할 조건)은 $4^2 \equiv 1 \mod 2$.
         - **케일리 판별법.** 일반적으로 $(a, b : a^n = 1, b^m = 1, ba = a^r b)$가 군일 필요충분조건은 $r^m \equiv 1 \mod n$.
4. 따라서 크기 10인 군은 순환군 $\mathbb{Z}_{10}$과 정이면체군 $D_5 = (a, b: a^5 = 1, b^2 = 1, ba = a^4 b)$, 2개임.