Thm | m과 n이 서로 소이면 $\mathbb{Z}_m \times \mathbb{Z}_n \simeq \mathbb{Z}_{mn}$ 이다.

(pf) Claim) m과 n이 서로 소이면 $\mathbb{Z}_m \times \mathbb{Z}_n$ 이 순환군이다.

Conjecture) $|\langle(1,1)\rangle| = \operatorname{lcm}(m,n)$

Conjecture 를 이용하면, $|\langle(1,1)\rangle| = \operatorname{lcm}(m,n) = mn$

Thm | m과 n이 서로 소가 아니면 $\mathbb{Z}_m \times \mathbb{Z}_n \not\simeq \mathbb{Z}_{mn}$

(pf) Claim) $|\langle(a,b)\rangle| < mn$

$(\because\ |\langle(a,b)\rangle| = \operatorname{lcm}(r_1, r_2)$ $\left(\begin{array}{l} r_1 : a\text{의 위수} \\ r_2 : b\text{의 위수} \end{array} \right)$

$\leq \operatorname{lcm}(m,n)$

$< mn$ m.n이 서로소 아니므로

28강 11절 3 : 유한생성 가환군 정리

Corol 11.6 | m_i 중 어느 두개를 선택해도 서로 소이면

$\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_n} \simeq \mathbb{Z}_{m_1 m_2 \cdots m_n}$ 이다.

(pf) 두개만 합칠 수 있음을 이용!

$\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_n}$

$= \mathbb{Z}_{m_1 m_2} \times \mathbb{Z}_{m_3} \times \cdots \times \mathbb{Z}_{m_n}$

$= \mathbb{Z}_{m_1 m_2 m_3} \times \mathbb{Z}_4 \times \cdots \times \mathbb{Z}_{m_n}$

$= \cdots = \mathbb{Z}_{m_1 m_2 \cdots m_n}$.

Corol | p_i 가 서로 다른 소수이고 $n = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$ 이라 하자.

그러면 $\mathbb{Z}_n \simeq \mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \cdots \times \mathbb{Z}_{p_r^{n_r}}$ 이다.

유한생성 가환군 (Finitely generated abelian group)

Thm 11.12 유한생성 가환군의 기본정리

모든 유한생성가환군 G는

$$\mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \cdots \times \mathbb{Z}_{p_n^{r_n}} \times \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{\text{Betti number}} \text{ 와 동형}$$

→ 여기서 p_i 들은 소수이고 서로 다를 필요는 없음.

r_i 들은 양의 정수

→ 직접곱은 인수들의 순서를 바꾸는 것을 무시하면 유일!

Def 유한생성가환군 G의 $\mathbb{Z}$ 의 개수를 the Betty number of G

(EX) 동형을 무시하고 위수가 360인 가환군을 모두 찾아라.

유한생성가환군의 기본정리에 의하여 G는 $\mathbb{Z}_m$ 또는 $\mathbb{Z}$ 의 직접곱이다.
→ G가 유한하기 때문에, G의 인수에 $\mathbb{Z}$는 존재하지 않는다.

(pf) 우선 360 소인수분해 $360 = 2^3 \times 3^2 \times 5$

$$\begin{aligned}
\mathbb{Z}_{360} &\simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 && (1)\\
&= \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 && (2)\\
&= \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 && (3)\\
&= \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5 && (4)\\
&= \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5 && (5)\\
&= \mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5 && (6)
\end{aligned}$$

29강 11절 4 : 분해가능군

• 분해 가능 vs 분해 불가능

Def 11.14 군 G가 2개의 비자명 진부분군들 (proper nontrivial subgroups) 의 직접곱과 동형이라면 decomposable group

→ 그렇지 않은 경우, G는 indecomposable group.

$\underbrace{G}_{\text{분해가능}} = \boxed{A} \times \boxed{B}$ $\quad A, B \neq \{e\}$ → $G = \{e\} \times G$

$6 = 2 \cdot 3$ 분해 가능

$7 = \underset{(e)}{1} \cdot 7$ 분해 불가능

Thm 11.15 decomposable 한 유한가환군은 소수의 멱 ($= p^r$ 꼴) 을 위수로 갖는 순환군 뿐. $\underbrace{\mathbb{Z}_{p_1^{r_1}}}_{\text{이런게 하나만 있는거지}} \times \mathbb{Z}_{p_2^{r_2}} \times \cdots$

(pf) G는 유한가환군이므로 $\mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}}$ ($k \geq 1$) 의 꼴로 쓸 수 있다.

(귀류법) 만약 G가 $\mathbb{Z}_{p^r}$ 꼴이 아니라면 $k \geq 2$ 이다.

→ $G = \mathbb{Z}_{p_1^{r_1}} \times (\cdots)$ 이므로 분해 가능 (→←)

⇒ 따라서 G는 $\mathbb{Z}_{p^r}$ 꼴이다 ∎

decomposable Group

* 라그랑지 정리 : 군 G의 부분군 H가 있으면 $|H| \mid |G|$ (즉 $H < G \Rightarrow |H| \mid |G|$)

Thm 11.16 만약 m이 유한가환군 G의 위수를 나눈다면 G는 위수 m인 부분군을 갖는다.

*** 보충설명** 유한가환군은 라그랑지 정리보다 더 강한 정리를 만족

$G = \mathbb{Z}_4 \times \mathbb{Z}_9$

* $|G| = 2^2 \cdot 3^2$ (p6)

1	$\{0\}$
3	$\langle 0 \rangle \times \langle 3 \rangle = \{(0,0), (0,3), (0,6)\}$
3^2	$\langle 0 \rangle \times \langle 1 \rangle = \{(0,0), (0,1), (0,2), (0,3), (0,4), (0,5), (0,6), (0,7), (0,8)\}$
2×1	$\langle 2 \rangle \times \langle 0 \rangle$
$2 \cdot 3$	$\langle 2 \rangle \times \langle 3 \rangle$
$2 \cdot 3^2$	$\langle 2 \rangle \times \langle 1 \rangle$
2^2	$\langle 1 \rangle \times \langle 0 \rangle$
$2^2 \cdot 3$	$\langle 1 \rangle \times \langle 3 \rangle$
$2^2 \cdot 3^2$	$\langle 1 \rangle \times \langle 1 \rangle$

* 4를 2로 나누어 2
9를 1로 나누면 9인데 $\mathbb{Z}_9$이므로 mod 9 = 0
↓
즉 나누어주면 generator 찾음

$G \simeq \mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}}$ (p_i는 소수이고 무조건 다를 필요 X)

$\Rightarrow |G| = p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k}$

$\Rightarrow m = p_1^{s_1} \cdots p_k^{s_k}$ ($s_i \le r_i$) 라 하자.

$H = \langle p_1^{r_1 - s_1}$

* Thm 11.16 이 라그랑지 정리와 차이점 ?

- In Lagrange Thm $|G| = 12 \Rightarrow$ 1, 2, 3, 4, 6, 12
  이 중에서 $|H|$를 고를수 있는 것
  위수 6인 군이 항상 존재? *Not ensure.*
- In Thm 11.16 $6 \mid \underset{12}{|G|} \Rightarrow$ 위수 6인 부분군이 존재 !
  이 크기를 갖는 부분군들이 다 존재.
  '유한생성가환군' 조건 때문.