Sylow Theorem

Date: Mar 13 Made by Eric

Definitions and Theorems

Definition 1. *Let G be a group, and F be a field. A* ***representation*** *ρ of G over F, is a homomorphism from G to $GL(F, n)$, and we say the* ***degree*** *$deg(\rho)$ of ρ is n.*

Definition 2. *ρ is* ***faithful*** *if $G \simeq \rho[G]$*

Definition 3. *Let G be a group, and F be a field, and ρ, σ be two representaion of G of the same degree. If $\exists T \in GL(F, n), \forall g \in G, T\rho(g)T^{-1} = \sigma(g)$, We call these two representations ρ, σ* ***equivalent****.*

Theorem 1. *Let $\rho \sim \sigma$ if ρ and σ are equivalent.*

$$\sim \text{ is an equivalence relation.}$$

Proof. $\forall g \in G, I\rho(g)I^{-1} = \rho(g) \implies g \sim g$ reflexivity

$\rho \sim \sigma \implies \exists Q \in GL(F, n), \forall g \in G, Q\rho(g)Q^{-1} = \sigma(g) \implies Q^{-1}\sigma(g)Q = \rho(g) \implies \sigma \sim \rho$ symmetry

$\rho \sim \sigma \sim \tau \implies \exists Q, T \in GL(F, n), \forall g \in G, Q\rho(g)Q^{-1} = \sigma(g)$ and $T\sigma(g)T^{-1} = \tau(g) \implies QT\rho(g)(QT)^{-1} = QT\rho(g)T^{-1}Q^{-1} = Q\sigma(g)Q^{-1} = \tau(g) \implies \rho \sim \tau$ transitivity

■

Theorem 2. *Let G be a group and F be a field. Let ϕ and ψ be two representation of G over F of the same degree.*

$$\phi \text{ is equivalent to } \psi \implies ker(\phi) = ker(\psi)$$

Proof. Let T be a matrix such that $\forall g \in G, T\phi(g)T^{-1} = \psi(g)$

$g \in ker(\phi) \iff \phi(g) = I_2 \iff T\phi(g)T^{-1} = I_2 \iff \psi(g) = I_2 \iff g \in ker(\psi)$

■

Exercises

1.

Proof. $(\longleftarrow)$

$\forall p, q : 0 \leq p, q \leq m - 1, \rho(a^p)\rho(a^q) = A^pA^q = A^{p+q} = A^c$, where $c \equiv_m p + q$

$\rho(a^p)\rho(a^q) = A^c = \rho(a^c) = \rho(a^p a^q)$

$(\longrightarrow)$

$A^m = \rho(a)^m = \rho(a^m) = \rho(e) = e$ ∎

2.

Proof. ρ_1 is a trivial homomorphism.

$$\rho_2(a)^3 = B^3 = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/3} \end{bmatrix}^3 = \begin{bmatrix} 1 & 0 \\ 0 & e^{6\pi i/3} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$
$$\rho_3(a^3) = C^3 = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}^3 = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$
$$\rho_2(a^2) = \begin{bmatrix} 1 & 0 \\ 0 & e^{4\pi i/3} \end{bmatrix} \neq I_2 \neq \rho_2(a)$$
$$\rho_3(a^2) = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix} \neq I_2 \neq \rho_3(a)$$

ρ_2 and ρ_3 are faithful. ∎

3.

Let ρ be the canonical homomorphism defined by $\rho(a) = 1$ and $\rho(b) = -1$

We now prove ρ satisfy the defining relation of D_4, so ρ is well defined.

$\rho(a)^n = 1^n = 1 = (-1)^2 = \rho(b)^2$

$\rho(b)^{-1}\rho(a)\rho(b) = (-1)^{-1}1(-1) = 1 = \rho(a)$ done

4.

Proof. This is Theorem 1 ∎

5.

Proof. Let $S = \{\rho_1, \rho_2, \rho_3, \rho_4\}$

We now prove ρ_1 is faithful

$$\rho(a^r b^0) = \begin{bmatrix} e^{r\frac{i\pi}{3}} & 0 \\ 0 & e^{-r\frac{i\pi}{3}} \end{bmatrix}$$

$\rho(a^r b) = \begin{bmatrix} 0 & e^{r\frac{i\pi}{3}} \\ e^{-r\frac{i\pi}{3}} & 0 \end{bmatrix}$

$\rho(a^r b^s) = I_2 \iff s = 0, r = 0$ done

We now prove ρ_2 is not faithful

$\rho_2(a^2 b^0) = \begin{bmatrix} e^{2i\pi} & 0 \\ 0 & e^{-2i\pi} \end{bmatrix} = I_2$ done

We now prove ρ_3 is not faithful

$\rho_3(a^3) = \begin{bmatrix} -e^{i\pi} & 0 \\ 0 & -e^{-i\pi} \end{bmatrix} = I_2$ done

We now prove ρ_4 is faithful

$\rho(a^2) = \begin{bmatrix} \frac{-1}{2} & \frac{\sqrt{3}}{2} \\ \frac{-\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix}$

$\rho(a^3) = -I_2$

$\rho(a)^6 = I_2$ and $\rho(a)^2 \neq I_2 \neq \rho(a)^3 \implies ord(\rho(a)) = 6$

$\rho(a^r b) = I_2 \iff \rho(a^r) \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \iff \rho(a^r) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

Let $E = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

$\rho(a^3) = -I_2 \implies \rho(a^4) = -\rho(a) \neq E \neq -\rho(a^2) = \rho(a^5) \implies \rho(a^r b) \neq I_2$
done

ρ_1, ρ_4 are faithful while ρ_2, ρ_3 are not.

If any of them are equivalent, then it must be ρ_1 equivalent to ρ_4, or ρ_2 equivalent to ρ_3

ρ_2 is not equivalent to ρ_3 since $a^2 \in ker(\rho_2) \setminus ker(\rho_3)$

Whether ρ_1 and ρ_4 are equivalent is left to prove

∎

6.

Proof. Let $D_4 = \langle a, b | a^4 = b^2 = 1, bab = a^{-1} \rangle$

Let ϕ be a representation of D_4 defined by lifting $\phi(a) = \begin{bmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ and $\phi(b) =$

$\begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ to the whole group.

■

7.

Proof. $\phi[G] \subseteq GL(1, F) \implies \phi[G]$ is abelian,

$\phi[G] \simeq G/ker(\phi) \implies G/ker(\phi)$ is abelian. ■

8.

Proof. No. $\phi(g)\phi(h) = \phi(h)\phi(g) \iff \phi(gh) = \phi(hg)$, gh and hg can be in the same coset of $\ker(\phi)$, yet not being the same element.

An example is when ϕ is a trivial representation. ■

Definitions and Theorems

Definition 4. *Let F be a field, and G be a group. A FG-**module** $F[G]$ is a vector space V over F, and a G-set at the same time, on which every elements $g \in G$ have action on V that is a linear transformation.*

Definition 5. *A **trivial** FG-module V is defined by $g(v) = v$. A **faithful** FG-module V satisfy $\forall v \in V, gv = v \implies g = e$*

Definition 6. *Two FG-module V, V' are equivalent if they are of same dimensional, and $\forall v \in V$,*

Definition 7. *Let G be a group. A **left** G-**module**, is an abelian group M, at the same time being a G-set, and satisfy*

$$\forall g \in G, \forall m, n \in M, g(m + n) = gm + gn$$

Definition 8. *Let $R = R^1$*

*A **left** R-**module**, is a left G-module, where G is the additive group of R, and satisfy the following more*

$$\forall r, s \in R, \forall m \in M, r(sm) = (rs)m \text{ and } \forall m \in M, 1m = m$$

Definition 9. *Let V be an FG-module, and β be a basis of V. For each $g \in G$, $[g]_\beta$ is the matrix of the action of g to the respect of β*

Theorem 3. ***(representation give rise to a module)*** *Let G be a group, and F be a field. Let ρ be a representation of G over F, of degree n. Let $V = F^n$, and a G-set defined by $\forall v \in V, \forall g \in G, g(v) = \rho(g)v$*

V is a $FG-M$, and for all basis β of V, $[g]_\beta = [\rho(g)]_\beta$

Proof. $\forall v \in V, ev = \rho(e)v = I_n v = v$

$\forall v \in V, g, h \in G, (g(hv)) = g(\rho(h)v) = \rho(g)(\rho(h)v) = \rho(g)\rho(h)v = \rho(gh)v = (gh)v$ The group G action on V is well defined

$\forall v \in V, \forall g \in G, \forall c \in F, c(gv) = c\rho(g)v = \rho(g)cv = g(cv)$

$\forall v, u \in V, \forall g \in G, g(u+v) = \rho(g)(u+v) = \rho(g)u + \rho(g)v = gu + gv$ every action is a linear transformation

$\forall v \in V, g(v) = (\rho(g))v \implies \forall v \in V, [g(v)]_\beta = [\rho(g)v]_\beta \implies \forall v \in V, [g]_\beta[v]_\beta = [\rho(g)]_\beta[v]_\beta \implies \forall i : 1 \le i \le n, ([g]_\beta)_i = ([\rho(g)]_\beta)_i \implies [g]_\beta = [\rho(g)]_\beta$ ∎

Theorem 4. ***(module give rise to some representation)*** *Let V be a FG-module, and β be a basis of V. Let $\rho : G \to GL(F, n)$ be defined by $\rho(g) = [g]_\beta$*

ρ is a representation of G

Proof. $\rho(g)\rho(h) = [g]_\beta[h]_\beta = [gh]_\beta = \rho(gh)$ ∎

Theorem 5. ***(The representations a FG-module give rise to are equivalent)*** *Let V be a FG-module, of which α, β are two distinct bases. Let ψ and ρ respectively be the representations defined by $\psi(g) = [g]_\alpha$ and $\rho(g) = [g]_\beta$*

ψ is equivalent to ρ

Proof. $\forall g \in G, [I_V]_\alpha^\beta \psi(g)([I_V]_\alpha^\beta)^{-1} = [I_V]_\alpha^\beta [g]_\alpha [I_V]_\beta^\alpha = [g]_\beta = \rho(g)$ ∎

Theorem 6. ***(there is a one-to-one correspondence between equivalent classes of representation and FG-module)*** *Let V be a FG-module, of which α is a basis, Let ψ be a representation of G defined by $\psi(g) = [g]_\alpha$, and ρ be a representation of G equivalent to ψ*

There exists a basis β such that $\rho(g) = [v]_\beta$

Proof. Let T be the matrix such $\forall g \in G, T\psi(g)T^{-1} = \rho(g)$

So $\rho(g) = T\psi(g)T^{-1} = T[g]_\alpha T^{-1}$

Let $\beta = \{T_1\}$ ∎

Theorem 7. *Let F be a field, G be a group, and V be a vector space, of which $\beta = \{\beta_1, \dots, \beta_n\}$ is a basis. Arbitrarily define $g(\beta_i)$, for all g and $\beta_i \in \beta$. Let $\forall g \in G, \forall v \in V : v = \sum_{i=1}^n c_i\beta_i, \exists\{c_1, \dots, c_n\}, g(v) = \sum_{i=1}^n c_i g(\beta_i)$*

V is a FG-space

Proof. Left to prove ∎