

5.4.1

Claim: If $|G| = p^3$ where p is prime, either $|Z(G)| = p$ or G is abelian.

Proof: Since we know

$$|G| = |Z(G)| + \sum_g \frac{|G|}{|\text{Cent}(g)|}$$

by class equation. Then by plugging in $|G| = p^3$, we get

$$p^3 = |Z(G)| + \sum_g \frac{p^3}{|\text{Cent}(g)|}.$$

Consider every subgroup has order a power of p by Lagrange's theorem, we know p divides $|Z(G)|$.

If $|Z(G)| = p$, the claim is proved.

If $|Z(G)| = p^3 = |G|$, then $Z(G) = G$, then G is abelian. If $|Z(G)| = p^2$, by Fundamental Theorem of Finitely Generated Abelian Group, we know that $Z(G) \cong \mathbb{Z}_{p^2}$ or $Z(G) \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

If $Z(G) \cong \mathbb{Z}_{p^2}$, $Z(G)$ is cyclic so G is abelian is true.

Since $\mathbb{Z}_p \times \mathbb{Z}_p$ is not abelian, $Z(G) \cong \mathbb{Z}_p \times \mathbb{Z}_p$ is impossible.

Thus, it is true that If $|G| = p^3$ where p is prime, either $|Z(G)| = p$ or G is abelian. ■

5.4.3

Claim: Let P be a p -Sylow subgroup of a finite group G . Let H be a subgroup of $N_G(P)$ such that $|H| = p^s$, then $H \subseteq P$.

Proof: Since P is a p -Sylow subgroup of a finite group G , $|G| = p^k m$ and $p \nmid m$, while $|P| = p^k$ and $P \subseteq G$. And from H is a subgroup of $N_G(P)$, we know $H \subseteq N_G(P) = \{g \in G | gPg^{-1} = P\} \subseteq G$ with $|H| = p^s$.

Since we have proved that $HP \subseteq N_G(P)$ and

$$|HP| = \frac{|P||H|}{|P \cap H|} \Leftrightarrow |H| = \frac{|P|}{|P \cap H| |HP|} < 1$$

So we know $|H| = p^s \leq p^k = |P| \Rightarrow p^s |p^k$.

Thus, we have $H \subseteq P$ by Corollary 5.4.5. ■

5.4.11

Claim: $|D_{14}| = |D_7 \times \mathbb{Z}_2| = 28$ with 2-Sylow subgroups isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $D_{14} \cong D_7 \times \mathbb{Z}_2$.

Proof: $|D_{14}| = 2 \cdot 14 = 28$, $|D_7 \times \mathbb{Z}_2| = 2 \cdot 7 \cdot 2 = 28$. Since $28 = 2 \cdot 2 \cdot 7$, let P be the 2-Sylow subgroup, $|P| = 4$. Since there're no elements of order 4 in D_{14} or $D_7 \times \mathbb{Z}_2$, so it can't be \mathbb{Z}_4 .

As a result, the 2-Sylow subgroups isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

We can construct a mapping $\varphi : D_{14} \rightarrow D_7 \times \mathbb{Z}_2$ by $e_{D_{14}} \mapsto (e_{D_7}, e_{\mathbb{Z}_2})$, $r_{D_{14}} \mapsto (r_{D_7}, e_{\mathbb{Z}_2})$, $a_{D_{14}} \mapsto (e_{D_7}, a_{\mathbb{Z}_2})$, which is a bijection so that $\varphi(e_{D_{14}} a_{D_{14}}) = \varphi(a_{D_{14}}) = (e_{D_7}, a_{\mathbb{Z}_2}) = (e_{D_7}, a_{\mathbb{Z}_2})(e_{D_7}, e_{\mathbb{Z}_2}) = \varphi(e_{D_{14}}) \varphi(a_{D_{14}})$, $\varphi^{14}(r_{D_{14}}) = ((r_{D_7}, e_{\mathbb{Z}_2}))^{14} = (r_{D_7}^{14}, e_{\mathbb{Z}_2}^{14}) = (e_{D_7}, e_{\mathbb{Z}_2}) = \varphi(r_{D_{14}}^{14})$, $\varphi^2(a_{D_{14}}) = (e_{D_7}, a_{\mathbb{Z}_2})^2 = (e_{D_7}^2, a_{\mathbb{Z}_2}^2) = (e_{D_7}, e_{\mathbb{Z}_2}) = \varphi(a_{D_{14}}^2)$ can be verified.

As a result, $D_{14} \cong D_7 \times \mathbb{Z}_2$. ■

6.1.5

Claim:

1. The set of matrices with integer entries is a subring of the ring of all n -by- n matrices with real entries.
2. The set of matrices with entries in \mathbb{N} is closed under addition and multiplication but is not a subring.

Proof: The additive and multiplicative closure, associativity and additive identity of the set of matrices with integer entries are guaranteed by the additive and multiplicative closure of integers. \mathbb{Z} is an abelian group, so the set of matrices with integer entries is also commutative. As a result, the set of matrices with integer entries is an abelian group. And since we know the set of matrices is multiplicatively associative and distributive, the set of matrices with integer entries is proved to be a ring.

Since $\mathbb{Z} \subseteq \mathbb{R}$, $\text{GL}(n, \mathbb{Z}) \subseteq \text{GL}(n, \mathbb{R})$.

Thus, it is proved that The set of matrices with integer entries is a subring of the ring of all n -by- n matrices with real entries.

Since for any matrix with entries in \mathbb{N} , although they are closed under addition and multiplication, but they do not have correspondent inverse, so it can't even form a group. So it can't be a subring. ■

6.1.6

Claim: The set of symmetric polynomials in three variables is a subring of the ring of all polynomials in three variables.

Proof: Since we know that the set of symmetric polynomials in three variables is a subset of the set of all polynomials in three variables, we only need to prove that the set of symmetric polynomials in three variables is a ring.

First of all, the additive and multiplicative associativity, additive commutativity and distributability are guaranteed because all polynomials in three variables is a ring.

Denote an arbitrary symmetric polynomials in three variables as $P[x, y, z] = g(x) + g(y) + g(z) + h(xy) + h(yz) + h(xz) + f(xyz)$, then it's easy to verify that $P[x_1, y_1, z_1] + P[x_2, y_2, z_2] = P[x_1 + x_2, y_1 + y_2, z_1 + z_2]$ is still a symmetric polynomial in three variables.

As a result, the set of symmetric polynomials in three variables is a ring and, thus, the set of symmetric polynomials in three variables is a subring of the ring of all polynomials in three variables. ■