25 End of groups of order p^3 (11/20)

25.1 Groups of order p^3

Lemma 25.1. *Let p be an* odd *prime number. Suppose that G is a non-abelian group of order p^3. If G has an element of order p^2, then G is isomorphic to a semi-direct product $\mathbf{Z}/p^2 \rtimes_\varphi \mathbf{Z}/p$.*

Proof. We assume that G has an element of order p^2. How many elements of order p^2 does G have? In this case, the homomorphism of Lemma 24.2 from $G \to Z(G)$ is surjective. The elements of order p^2 are the elements $x \in G$ such that x^p is not the identity element in $Z(G)$ under the homomorphism of Lemma 24.2. There are $(p-1)$ non-identity elements in the image and each of them is hit by p^2 elements since the kernel of $G \to Z(G)$ has order p^2. Thus, there are $p^3 - p^2$ elements of order p^2. There are therefore $p^2 - 1$ elements of order p.

Choose an element x of order p^2. Then, x generates a subgroup N of G isomorphic to $\mathbf{Z}/p^2$. In fact, N is normal. Indeed, N must contain $Z(G)$ since otherwise N and $Z(G)$ would generate G and G would be abelian. Thus, N is the inverse image of some subgroup of $G/Z(G)$. But, $G/Z(G)$ is a group of order p^2 (isomorphic to $\mathbf{Z}/p \times \mathbf{Z}/p$) and is thus abelian, so every subgroup is normal, and then N is normal. Thus, G fits into an exact sequence

$$1 \to \mathbf{Z}/p^2 \to G \to \mathbf{Z}/p \to 1.$$

To complete the proof, we have only to see that the sequence is split. But, N contains only $p-1$ elements of order p. Since there are $p^2 - 1$ elements of order p, some of them are not in N and thus the sequence is split, as desired. □

Proposition 25.2. *Let p be an* odd *prime number. Up to isomorphism, there is a unique non-abelian group of order p^3 with an element of order p^2. It is isomorphic to $\mathbf{Z}/p^2 \rtimes_\varphi \mathbf{Z}/p$ where $\varphi\colon \mathbf{Z}/p \to \mathrm{Aut}(\mathbf{Z}/p^2) \cong \mathbf{Z}/(p(p-1))$ is any non-trivial homomorphism.*

Proof. Existence follows from the computation of $\mathrm{Aut}(\mathbf{Z}/p^2)$. Uniqueness follows from an argument similar to the proof of Proposition 22.1. □

Proposition 25.3. *Let p be an* odd *prime number. Up to isomorphism, there is a unique non-abelian group of order p^3 with no elements of order p^2.*

Proof. As $\mathrm{Aut}(\mathbf{Z}/p \times \mathbf{Z}/p) \cong \mathbf{GL}_2(\mathbf{F}_p)$ has order $(p-1)^2 p(p+1)$, there is a non-trivial homomorphism $\varphi\colon \mathbf{Z}/p \to \mathbf{GL}_2(\mathbf{F}_p)$ and hence there is a semi-direct product $(\mathbf{Z}/p \times \mathbf{Z}/p) \rtimes_\varphi \mathbf{Z}/p$ which is non-abelian.

Suppose that G is a non-abelian group of order p^3 with no elements of order p^2. Then, the inverse image of any subgroup of the form $\mathbf{Z}/p$ in $G \to G/Z(G) \cong \mathbf{Z}/p \times \mathbf{Z}/p$ is a normal subgroup of G isomorphic to $\mathbf{Z}/p \times \mathbf{Z}/p$ (and contains the center). Thus, G fits into an extension

$$1 \to \mathbf{Z}/p \times \mathbf{Z}/p \to G \to \mathbf{Z}/p \to 1.$$

Since every element of G has order 1 or p, the extension is split, and G is a semi-direct product, as above.

Uniqueness is left to the reader as Exercise 25.2, which shows that any two non-trivial semi-direct products are isomorphic. (This part works for $p = 2$ as well.)

The last thing to prove is that some such semi-direct product has no elements of order p^2. However, the pth power homomorphism $G \to Z(G)$ must send all of $\mathbf{Z} \times \mathbf{Z}$ to the identity and thus it factors through $G/(\mathbf{Z}/p \times bZ/p) \cong \mathbf{Z}/p$. However, since the extension is split, we see that this factorization is also trivial. More precisely, letting $f''\colon G/(\mathbf{Z}/p \times \mathbf{Z}/p) \to Z(G)$ be the factorization, we have that $f'' = f \circ g$ where $g\colon \mathbf{Z}/p \to G$ is a splitting of the exact sequence. But, the image of g consists of elements of order dividing p. □

Example 25.4 (Groups of order p^3 for odd primes p)**.** It follows from the results above that, up to isomorphism, there are 5 groups of order p^3 if p is an odd prime. The one from Proposition 25.3 is called the **Heisenberg group** He_p.

25.2 Remark on semi-direct products of the form $p^\alpha q^\beta$

Remark 25.5. Let G be a finite group of order $p^\alpha q^\beta$ where $p < q$. If G has a normal Sylow subgroup, then it is a semi-direct product. Sometimes, this is guaranteed. This is the case for example when p^γ is not congruent to 1 mod q for any $1 \leqslant \gamma \leqslant \alpha$, or when q^γ is not congruent to 1 mod p for any $1 \leqslant \gamma \leqslant \beta$.

25.3 Exercises

Exercise 25.1. Find a subgroup of $\mathbf{GL}_2(\mathbf{Z}/p^2)$ isomorphic to the group of Proposition 25.2.

Exercise 25.2. Let p be a prime and let $\varphi_i \colon \mathbf{Z}/p \to \mathbf{GL}_2(\mathbf{F}_p)$ be non-trivial homomorphisms for $i = 1, 2$. Show that the corresponding semi-direct products $(\mathbf{Z}/p \times \mathbf{Z}/p) \rtimes_{\varphi_i} \mathbf{Z}/p$ are isomorphic.

Exercise 25.3. Let p be a prime number and consider the group $\mathbf{U}_3(\mathbf{F}_p)$ of Example 19.2. This is a non-abelian group of order p^3. Describe it as a semi-direct product and, when p is odd, determine whether it has an element of order p^2 or not.

Exercise 25.4. Classify groups of order 63.

Exercise 25.5. Show that every group of order 1225 is abelian.