24 Groups of order p^3 (11/17)

Remark 24.1. If p is a prime number and G is a non-abelian group of order p^3, then there are $p+1$ proper subgroups of $G/Z(G) \cong \mathbf{Z}/p \times \mathbf{Z}/p$, each isomorphic to $\mathbf{Z}/p$. Pulling back along $G \to G/Z(G)$, we see that there are $p+1$ subgroups of order p^2 inside G; each contains $Z(G)$. There are two cases to analyze: (a) when one of these subgroups is isomorphic to $\mathbf{Z}/p^2$ and (b) when all of these subgroups are isomorphic to $\mathbf{Z}/p \times \mathbf{Z}/p$.

Lemma 24.2. *Let G be a group of order p^3 where p is an* odd *prime number. The pth power function $f\colon G \to G$ given by $f(x) = x^p$ is a group homomorphism. Moreover, the kernel of f contains $Z(G)$ and the image of f is contained in $Z(G)$, so f induces a homomorphism $f'\colon G/Z(G) \to Z(G)$.*

Proof. We want to show that $f(xy) = f(x)f(y)$ for any $x, y \in G$. Claim: x and y commute with $[x,y]$. Indeed, $[x,y]$ maps to the identity element in $G/Z(G)$ since this group is abelian. Thus, $[x,y]$ is in $Z(G)$ and hence commutes with all elements of G. It follows from Exercise 24.1 that $f(xy) = (xy)^p = x^p y^p [y,x]^{\frac{p(p-1)}{2}} = f(x)f(y)$, as p divides $\frac{p(p-1)}{2}$ and $[y,x]$ has order dividing p. $\square$

Definition 24.3. Let G be a finite group. The exponent of G is the smallest integer n such that $x^n = e$ for all $x \in G$. It is the least common multiple of the orders of all elements of G and it divides $|G|$.

Example 24.4. If G is a non-abelian group of order p^3 where p is a prime number, then G has exponent p or p^2.

The following results will be proved next time.

Lemma 24.5. *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 $\mathbf{Z}/p^2 \rtimes_\varphi \mathbf{Z}/p$.*

Proposition 24.6. *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.*

Proposition 24.7. *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.*

Example 24.8 (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 24.7 is called the **Heisenberg group** He_p.

Example 24.9 (Groups of order 8)**.** Something funny happens for $p = 2$. The two non-trivial semi-direct products

$$\mathbf{Z}/4 \rtimes \mathbf{Z}/2 \quad \text{and} \quad (\mathbf{Z}/2 \times \mathbf{Z}/2) \rtimes \mathbf{Z}/2$$

are isomorphic. Indeed, one sees that the dihedral group D_8 can be described as a semi-direct product in both ways. So, it seems like there might only by 4 isomorphism classes of groups of order 8. However, there is another group, the quaternion group Q_8, which we discuss next.

Example 24.10 (The quaternions)**.** We denote by Q_8 the set $\{1, -1, i, -i, j, -j, k, -k\}$ and define a binary operation as $1 \cdot x = x$, $(-1)^2 = 1$, $(-1) \cdot x = -x$, $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -jk = i$, and $ki = -ik = j$. These imply that $ijk = -1$ as well. It is straightforward to see that this defines a binary operation with inverses and an identity element. Associativity is cumbersome to prove directly. However, we can find elements in $\mathbf{GL}_2(\mathbf{C})$ satisfying the same relations:

$$\pm 1 = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \pm i = \pm \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \pm j = \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \pm k = \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

These satisfy the same relations and since matrix multiplication is associative, so is the binary operation on Q_8.

24.1 Exercises

Exercise 24.1. Let G be a group and $x, y \in G$ elements which both commute with $[x, y] = xyx^{-1}y^{-1}$. Show that for each $n \geqslant 1$, the equality $(xy)^n = x^n y^n [y, x]^{\frac{n(n-1)}{2}}$ holds.

Exercise 24.2. Show that Q_8 is not a non-trivial semi-direct product.

Exercise 24.3. Show that any non-abelian group of order 8 is isomorphic to D_8 or Q_8.