22 Groups of small order (11/15)

22.1 Groups of order pq

Proposition 22.1. *Suppose that p and q are primes and that p divides $q-1$. There is a unique non-abelian group of order pq up to isomorphism.*

Proof. We have seen most of the proof in the course of Example 22.5. In particular, we have seen that any such group is a semi-direct product $\mathbf{Z}/q \rtimes_\varphi \mathbf{Z}/p$ for *some* $\varphi\colon \mathbf{Z}/p \to \mathrm{Aut}(\mathbf{Z}/q)$ and that there are non-trivial such φ. The only thing that remains to be seen is uniqueness. There are $p-1$ choices of a non-trivial homomorphism $\varphi\colon \mathbf{Z}/p \to \mathrm{Aut}(\mathbf{Z}/q)$, corresponding to the $p-1$ choices of an element of order p in $\mathrm{Aut}(\mathbf{Z}/q) \cong (\mathbf{Z}/q)^\times \cong \mathbf{Z}/(q-1)$. Suppose that φ_0 and φ_1 are two such homomorphism, corresponding to elements $k_0, k_1 \in (\mathbf{Z}/q)^\times$. In particular, there is some integer $c \in \{1, \ldots, p-1\}$ such that $k_1^c = k_0$ since they generate the same subgroup. In particular, $c \in (\mathbf{Z}/p)^\times$. Let $G_0 = \mathbf{Z}/q \rtimes_{\varphi_0} \mathbf{Z}/p$ and $G_1 = \mathbf{Z}/q \rtimes_{\varphi_1} \mathbf{Z}/p$. Define a function $f\colon G_0 \to G_1$ as follows. Of course, as sets, both G_0 and G_1 are $\mathbf{Z}/q \times \mathbf{Z}/p$. So, write an element as (a, b). We let

$$f(a, b) = (a, cb).$$

Now, we check that this defines a group homomorphism. On the one hand,

$$f(x_0, y_0)f(x_1, y_1) = (x_0, cy_0) \cdot_{G_1} (x_1, cy_1) = (x_0 + k_1^{cy_0} x_1, cy_0 + cy_1) = (x_0 + k_0^{y_0}, c(y_0 + y_1))$$

since $k_1^{cy_0} = k_0^{y_0}$, and on the other hand

$$f((x_0, y_0) \cdot_{G_0} (x_1, y_1)) = f(x_0 + k_0^{y_0} x_1, y_0 + y_1) = (x_0 + k_0^{y_0}, c(y_0 + y_1)).$$

It follows that f is a group homomorphism. As $c \in (\mathbf{Z}/p)^\times \cong \mathrm{Aut}(\mathbf{Z}/p)$, it is an isomorphism, with inverse $g(a, b) = (a, db)$ where $cd \equiv 1 \mod p$. This completes the proof. ☐

Example 22.2. There are no non-abelian groups of order 33.

Example 22.3. There is a unique (up to isomorphism) non-abelian group of order 57.

22.2 A group of order $(q-1)q$

Example 22.4. A kind of maximal semi-direct product of something something by a group N is given by

$$1 \to N \to N \rtimes_{\mathrm{id}} \mathrm{Aut}(N) \to \mathrm{Aut}(N) \to 1,$$

where we use the identity homomorphism $\mathrm{Aut}(N) \xrightarrow{\mathrm{id}} \mathrm{Aut}(N)$ for the "action" homomorphism. In the case when $N = \mathbf{Z}/q$ for a prime q, we know that $\mathrm{Aut}(N) = \mathrm{Aut}(\mathbf{Z}/q) \cong (\mathbf{Z}/q)^\times \cong \mathbf{Z}/(q-1)$ is cyclic, so we get a semi-direct product

$$1 \to \mathbf{Z}/q \to \mathbf{Z}/q \rtimes \mathbf{Z}/(q-1) \to \mathbf{Z}/(q-1) \to 1.$$

By construction, if p divides q, then there is a homomorphism $\varphi\colon \mathbf{Z}/p \to \mathbf{Z}/(q-1)$ and hence a group homomorphism $\mathbf{Z}/q \rtimes_\varphi \mathbf{Z}/p \to \mathbf{Z}/q \rtimes \mathbf{Z}/(q-1)$.

Warning 22.5. These are not typically the only groups of order $(q-1)q$.

22.3 Groups of small order checklist

$\lvert G \rvert$		known groups	complete?	simple group?
2	p	$\mathbf{Z}/2$	x	x
3	p	$\mathbf{Z}/3$	x	x
4	p^2	$\mathbf{Z}/4$, $(\mathbf{Z}/2)^2$	x	o
5	p	$\mathbf{Z}/5$	x	x
6	pq	S_3, $\mathbf{Z}/6$	x	o
7	p	$\mathbf{Z}/7$	x	x
8	p^3	D_8, $\mathbf{Z}/8$, $\mathbf{Z}/4 \times \mathbf{Z}/2$, $(\mathbf{Z}/2)^3$	o	o
9	p^2	$\mathbf{Z}/9$, $(\mathbf{Z}/3)^2$	x	o
10	pq	D_{10}, $\mathbf{Z}/10$	x	o
11	p	$\mathbf{Z}/11$	x	x
12	p^2q	$\mathbf{Z}/12$, $\mathbf{Z}/6 \times \mathbf{Z}/2$, D_12	o	o

22.4 Groups of order p^3

Example 22.6. Let p be a prime number. Up to isomorphism, there are three abelian groups of order p^3. They are $\mathbf{Z}/p^3$, $\mathbf{Z}/p^2 \times \mathbf{Z}/p$, and $\mathbf{Z}/p \times \mathbf{Z}/p \times \mathbf{Z}/p$.

Lemma 22.7. *Let p be a prime number. If G is a non-abelian group of order p^3, then the center $Z(G)$ of G has order p.*

Proof. Since G is a p-group, its center is non-trivial, and thus has order p, p^2, or p^3. However, G is abelian, so $Z(G) \neq G$ and thus the center has order p or p^2. Suppose the center of G has order p^2. It is a normal subgroup of G and $G/Z(G)$ has order p and is thus isomorphic to $\mathbf{Z}/p$. Let $x \in G$ map to $1 \in \mathbf{Z}/p$. Let $y \in Z(G)$. Then, $xy = yx$ since y is in the center. There are p^3 elements of the form $x^i y$ for $i \in \{0, \ldots, p-1\}$ and $y \in Z(G)$. Thus, every element of G is of this form. As x commutes with all of these elements, it follows that x is in the center of G, so that $Z(G) = G$, a contradiction. $\square$

Lemma 22.8. *Let p be a prime number. Suppose that G is a non-abelian group of order p^3. Then, every element of G has order 1, p, or p^2.*

Proof. The only thing to check is that there is no element of order p^3. If there were, there would be an injective group homomorphism $\mathbf{Z}/p^3 \to G$, which would be an isomorphism, in contradiction to the assumption that G is non-abelian. $\square$

Lemma 22.9. *Let p be a prime number. If G is a non-abelian group of order p^3, then $G/Z(G) \cong \mathbf{Z}/p \times \mathbf{Z}/p$.*

Proof. If not, then $G/Z(G) \cong \mathbf{Z}/p^2$. In this case, the corresponding extension

$$1 \to Z(G) \to G \to G/Z(G) \to 1$$

must be split, meaning just that a generator of $G/Z(G) \cong \mathbf{Z}/p^2$ lifts to an order p^2 element of G. (Otherwise, it would lift to an order p^3 element and G would be abelian, a contradiction.) Thus, G is a semi-direct product $\mathbf{Z}/p \rtimes \mathbf{Z}/p^2$. But, as there are no non-trivial homomorphisms $\mathbf{Z}/p^2 \to \mathrm{Aut}(\mathbf{Z}/p) \cong (\mathbf{Z}/p)^\times$, it follows that G is the product $\mathbf{Z}/p \times \mathbf{Z}/p^2$ and is abelian, a contradiction. $\square$

22.5 Exercises

Exercise 22.1. Suppose that $p < q$ are primes and that $p \mid (q-1)$. Prove that there is a non-abelian subgroup of $\mathbf{GL}_2(\mathbf{F}_q)$ of order pq by writing down explicit conditions on 2×2-matrices, checking that these conditions define a subgroup, and counting the resulting elements.

Exercise 22.2. Find 10 triples $p < q < r$ of prime numbers such that every group of order pqr is abelian.