22 Groups of order pq (11/13)

We need the following theorem as a black box.

Theorem 22.1. *If p is a prime number, then $(\mathbf{Z}/p)^\times$ is cyclic.*

Proof. This proof will be given in the second or third quarters of this course. $\square$

Remark 22.2. It turns out that $(\mathbf{Z}/p)^\times$ is isomorphic to the group of elements of the complex plane $\mathbf{C}$ of the form $e^{\frac{2\pi k}{p-1}}$ where $k = 0, \ldots, p-2$. I do not know of a truly elementary proof of Theorem 22.1, i.e., which does not use certain polynomials in a crucial way.

Corollary 22.3. *If p is a prime number, then $(\mathbf{Z}/p)^\times \cong \mathbf{Z}/(p-1)$.*

Proof. We already know that $(\mathbf{Z}/p)^\times$ has $p-1$ elements; by Theorem 22.1, the corollary follows. $\square$

Example 22.4. We call an element $i \in (\mathbf{Z}/n)^\times$ a multiplicative generator if $(\mathbf{Z}/n)^\times$ is cyclic **and** it is generated by i. For example,

- $(\mathbf{Z}/3)^\times$ is multiplicatively generated by 2;
- $(\mathbf{Z}/5)^\times$ is multiplicatively generated by 2 or 8;
- $(\mathbf{Z}/7)^\times$ is multiplicatively generated by 3 or 5.

Example 22.5 (Groups of order pq)**.** Let $p < q$ be distinct primes. There is a unique abelian group of order pq, up to isomorphism, which is $\mathbf{Z}/(pq) \cong \mathbf{Z}/q \times \mathbf{Z}/p$. When is there a non-abelian group of order pq? This occurs if and only if $p \mid q-1$. Indeed, we know that a group G of order pq has a normal q-Sylow subgroup, say N, which is isomorphic to $\mathbf{Z}/q$. The quotient of G by N is isomorphic to $\mathbf{Z}/p$. So, G is an extension of $\mathbf{Z}/p$ by $\mathbf{Z}/q$. This extension is in fact split. Indeed, G has an element of order p which must map to a non-zero element of the quotient $\mathbf{Z}/p$. By Proposition 21.12, G is isomorphic to $\mathbf{Z}/q \rtimes_\varphi \mathbf{Z}/p$. Now, $\mathrm{Aut}(\mathbf{Z}/q)$ is a group of order $(q-1)$. If p does not divide $q-1$, then the only group homomorphism $\mathbf{Z}/p \to \mathrm{Aut}(\mathbf{Z}/q)$ is the identity and it follows, from Exercise 21.2, that in this case G is the product $\mathbf{Z}/q \times \mathbf{Z}/p$. On the other hand, if p does divide $(q-1)$, then by Cayley's theorem there is an element of $\mathrm{Aut}(\mathbf{Z}/q)$ of order p and hence a non-trivial homomorphism $\varphi\colon \mathbf{Z}/p \to \mathbf{Z}/q$. The associated semidirect product $\mathbf{Z}/q \rtimes_\varphi \mathbf{Z}/p$ is non-abelian.

Example 22.6. There are no non-abelian groups of order 15.

22.1 Exercises

Exercise 22.1. Find multiplicative generators of $\mathbf{Z}/11$ and $\mathbf{Z}/13$.

Exercise 22.2. Show that if p is a prime number, then $(\mathbf{Z}/p^2)^\times$ is cyclic.

Exercise 22.3. Find an integer $n > 1$ such that $(\mathbf{Z}/n)^\times$ is *not* cyclic.

Exercise 22.4. Make a list of the first 10 primes. Then, make a list of all products pq where p and q are on your list such that every group of order pq is abelian. For example, every group of order 15 is abelian.