ANALYSIS OF SMALL GROUPS

1. Big Enough Subgroups are Normal

Proposition 1.1. *Let G be a finite group, and let q be the smallest prime divisor of $|G|$. Let $N \subset G$ be a subgroup of index q. Then N is a normal subgroup of G.*

Proof. The group G acts on the coset space G/N by left translation, giving a map from G to the symmetric group on q letters,

$$G \longrightarrow \mathrm{Aut}(G/N) \approx S_q.$$

Let K denote the kernel of the map. Clearly $K \subset N$ since each $g \in K$ must in particular left translate N back to itself. Thus, since q is the smallest prime divisor of $|G|$,

$$q = |G/N| \mid |G/K| = q \cdot (\text{product of primes } p \geq q).$$

On the other hand, the first isomorphism theorem says that G/K is isomorphic to the image of G in S_q, a subgroup of S_q. Thus $|G/K| \mid q!$, so that

$$|G/K| = q \cdot (\text{product of primes } p < q).$$

Comparing the two displays shows that $|G/N| = |G/K|$, and so the containment $K \subset N$ now gives $K = N$. Thus N is normal because it is a kernel.

□

2. Semidirect Products

First we discuss what it means for a given group to be a semidirect product of two of its subgroups.

Let G be a group, let K be a normal subgroup, and let Q be a complementary subgroup. That is,

$$G = KQ, \quad K \lhd G, \quad K \cap Q = 1_G.$$

Define a map

$$\sigma : Q \longrightarrow \mathrm{Aut}(K), \quad q \longmapsto \big(\sigma_q : k \mapsto qkq^{-1}\big).$$

Thus $\sigma_{qq'} = \sigma_q \circ \sigma_{q'}$ for all $q, q' \in Q$, i.e., σ is a homomorphism. And of course $\sigma_q(kk') = \sigma_q(k)\sigma_q(k')$ for all $k, k' \in K$ since conjugation is an inner automorphism.

Then the group-operation of G is

$$kq \cdot \tilde{k}\tilde{q} = kq \cdot \tilde{k}q^{-1} \cdot q\tilde{q} = k\sigma_q(\tilde{k}) \cdot q\tilde{q}.$$

This group structure describes G as a **semidirect product** of K and Q. The notation is

$$G = K \times_\sigma Q.$$

When Q acts trivially on K by conjugation, i.e., when all elements of K and Q commute, the semidirect product is simply the direct product. Regardless of whether the semidirect product is direct, we have a **short exact sequence**

$$1 \longrightarrow K \longrightarrow G \longrightarrow Q \longrightarrow 1,$$

where the first map is inclusion and the second is $kq \mapsto q$. Furthermore, the sequence **splits**, in that the composite $Q \longrightarrow G \longrightarrow Q$, where the first map is inclusion, is the identity. The short exact sequence makes clear that K is so-named because it is the kernel group in the sequence, and similarly Q is so-named because it is the quotient group.

Second we discuss ingredients that suffice to *construct* a semidirect product.

Suppose that we have the data

- a group K,
- a group Q,
- a homomorphism $\sigma : Q \longrightarrow \mathrm{Aut}(K)$.

Define the following operation on the set $G = K \times Q$:

$$(k, q)(k', q') = (k\sigma_q(k'), qq').$$

Note that the operation does not assume any sort of product between elements of K and elements of Q.

The operation is associative,

$$\begin{aligned}((k, q)(k', q')) \cdot (k'', q'') &= (k\sigma_q(k'), qq') \cdot (k'', q'') \\ &= (k\sigma_q(k')\sigma_{qq'}(k''), (qq')q'') \\ &= (k\sigma_q(k'\sigma_{q'}(k'')), q(q'q'')) \\ &= (k, q) \cdot (k'\sigma_{q'}(k''), q'q'') \\ &= (k, q) \cdot ((k', q')(k'', q'')).\end{aligned}$$

The identity is $(1_K, 1_Q)$,

$$\begin{aligned}(k, q)(1_K, 1_Q) &= (k\sigma_q(1_K), q1_Q) = (k, q), \\ (1_K, 1_Q)(k, q) &= (1_K\sigma_{1_Q}(k), 1_Qq) = (k, q).\end{aligned}$$

And the inverse of (k, q) is $(\sigma_{q^{-1}}(k^{-1}), q^{-1})$,

$$\begin{aligned}(k, q)(\sigma_{q^{-1}}(k^{-1}), q^{-1}) &= (k\sigma_q(\sigma_{q^{-1}}(k^{-1})), qq^{-1}) = (1_K, 1_Q), \\ (\sigma_{q^{-1}}(k^{-1}), q^{-1})(k, q) &= (\sigma_{q^{-1}}(k^{-1})\sigma_{q^{-1}}(k), q^{-1}q) = (1_K, 1_Q).\end{aligned}$$

Thus G is a group.

If we identify K with its embedded image $K \times 1_Q$ in G and similarly identify Q with $1_K \times Q$ in G then the group operation becomes the semidirect product law,

$$kq \cdot k'q' = k\sigma_q(k')qq',$$

and K is normal,

$$(*, q)(k, 1_Q)(*, q)^{-1} = (*, q)(k, 1_Q)(*, q^{-1}) = (*, 1_Q).$$

Thus the data K, Q, and σ give a semidirect product construction $G = K \times_\sigma Q$ without assuming that K and Q are subgroups of a common group.

3. Groups of Order p^2

Let $|G| = p^2$ where p is prime, and let G act on itself by conjugation. The class formula gives

$$p^2 = |Z(G)| + \sum_{\mathcal{O}_x} p^2/|G_x|.$$

The sum is a multiple of p, and hence so is $|Z(G)|$. We are done unless $|Z(G)| = p$. In this case, consider a noncentral element g. Its isotropy group contains $Z(G)$ and g, making it all of G. This contradicts the noncentrality of g. Thus $|Z(G)| = p^2$, i.e., $Z(G) = G$, i.e., G is abelian.

4. Metacyclic Groups of Order pq

Let p and q be primes with $q > p$. We seek nonabelian groups G of order pq.

Any q-Sylow subgroup of G,

$$K = \{1, a, \cdots, a^{q-1}\},$$

is big enough to be normal. Thus, letting a p-Sylow subgroup be

$$Q = \{1, b, \cdots, b^{p-1}\},$$

we have

$$G = KQ, \quad K \lhd G, \quad K \cap Q = 1_G.$$

That is, G is a semidirect product of K and Q. The only question is how Q acts on K by conjugation.

The automorphisms of K are

$$a \longmapsto a^e \quad \text{for any nonzero } e \in \mathbb{Z}/q\mathbb{Z},$$

and the composition of $a \mapsto a^e$ and $a \mapsto a^f$ is $a \mapsto a^{ef}$. That is,

$$\mathrm{Aut}(K) \approx (\mathbb{Z}/q\mathbb{Z})^\times.$$

Elementary number theory (see below) shows that there is at least one *generator* g modulo q such that

$$\{1, g, g^2, g^3, \cdots, g^{q-2}\} \quad \text{gives all the values } 1, 2, 3, \cdots, q-1 \text{ modulo } q.$$

That is, $g^{q-1} = 1 \bmod q$ is the first positive power of g that equals 1 modulo q, so that

$$\mathrm{Aut}(K) \text{ is cyclic of order } q-1.$$

Therefore, there are nontrivial maps $\sigma : Q \longrightarrow \mathrm{Aut}(K)$ if and only if $p \mid q-1$. In this case, the unique order p subgroup of $\mathrm{Aut}(K)$ is isomorphic to

$$\{1, g^{(q-1)/p}, g^{2(q-1)/p}, g^{(p-1)(q-1)/p}\},$$

whose nontrivial elements are precisely the values $i \in \mathbb{Z}/q\mathbb{Z}$ such that $i \neq 1$ but $i^p = 1$. Thus the nontrivial maps $Q \longrightarrow \mathrm{Aut}(K)$ are

$$b \longmapsto \left(a \mapsto a^i\right), \quad i \neq 1 \bmod q \text{ but } i^p = 1 \bmod q.$$

In sum, nonabelian groups of order pq exist only for $p \mid q-1$, in which case they are

$$\left\langle a, b \,|\, a^q = b^p = 1,\ bab^{-1} = a^i \right\rangle \quad \text{where } i \neq 1 \bmod q \text{ but } i^p = 1 \bmod q.$$

Especially, if $p = 2$ then the only possibility is $i = -1 \bmod q$, giving the dihedral group D_q.

For a given p and q with $p \mid q-1$, different values of i give isomorphic groups. To see this, first note that any two such values i and i' satisfy

$$i' = i^e \bmod q \quad \text{for some } e \in \{1, \cdots, p-1\}.$$

Now let $\tilde{b} = b^e$. Then the relations $a^q = b^p = 1,\ bab^{-1} = a^i$ become

$$a^q = \tilde{b}^p = 1,\ \tilde{b}a\tilde{b}^{-1} = a^{i'}.$$

To see where the last relation comes from, compute

$$\begin{aligned} b^e a b^{-e} &= b^{e-1} \cdot bab^{-1} \cdot b^{-(e-1)} \\ &= b^{e-1} a^i b^{-(e-1)} \\ &= (b^{e-1} a b^{-(e-1)})^i \\ &= (b^{e-2} a b^{-(e-2)})^{(i^2)} \\ &= \cdots \\ &= a^{(i^e)}. \end{aligned}$$

Since $b^p = 1$, this same calculation with p in place of e shows again why we need $i^p = 1 \bmod q$, forcing p to divide $q - 1$.

In general, any semidirect product $K \times_\sigma Q$ where K and Q are cyclic (not necessarily of prime order) is called **metacyclic**.

4.1. **A Brief Excursion into Elementary Number Theory.** We have cited the following result.

Proposition 4.1. *Let q be prime. Then $(\mathbb{Z}/q\mathbb{Z})^\times$ is cyclic, with $\varphi(q-1)$ generators.*

An elementary proof is possible, and indeed it is standard. But we have the tools in hand to give a more sophisticated argument. First of all, if $(\mathbb{Z}/q\mathbb{Z})^\times$ is cyclic then our analysis of cyclic groups has already shown that it has $\varphi(q-1)$ generators. So only the cyclicity is in question.

The proof begins with the observation that a polynomial over a field can not have more roots than its degree.

Lemma 4.2. *Let k be a field. Let the polynomial $f \in k[X]$ have degree $d \geq 1$. Then f has at most d roots in k.*

Naturally, the field that we have in mind here is $k = \mathbb{Z}/q\mathbb{Z}$.

The lemma does require that k be a field, not merely a ring. For example, the quadratics polynomial $X^2 - 1$ over the ring $\mathbb{Z}/24\mathbb{Z}$ has eight roots,

$$\{1, 5, 7, 11, 13, 17, 19, 23\} = (\mathbb{Z}/24\mathbb{Z})^\times.$$

Proof. If f has no roots then we are done. Otherwise let $a \in k$ be a root. The polynomial division algorithm gives

$$f(X) = q(X)(X - a) + r(X), \quad \deg(r) < 1 \text{ or } r = 0.$$

(Here the quotient polynomial $q(X)$ is unrelated to the prime q in the ambient discussion.) Thus $r(X)$ is a constant. Substitute a for X to see that in fact $r = 0$, and so $f(X) = q(X)(X - a)$. By induction, q has at most $d - 1$ roots in k and we are done. ☐

Now, since $(\mathbb{Z}/q\mathbb{Z})^\times$ is a finite abelian group, it takes the form

$$(\mathbb{Z}/q\mathbb{Z})^\times \approx \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_k\mathbb{Z}, \qquad 1 < d_1 \mid d_2 \mid \cdots \mid d_k.$$

The additive description of the group shows that the equation $d_k X = 0$ is solved by all $d_1 d_2 \cdots d_k$ group elements. Multiplicatively, the polynomial

$$X^{d_k} - 1 \in (\mathbb{Z}/q\mathbb{Z})[X]$$

has $d_1 d_2 \cdots d_k$ roots. Thus $k = 1$ and so $(\mathbb{Z}/q\mathbb{Z})^\times$ is cyclic.

5. Groups of Order 8

Let G be a nonabelian group of order 8. Then G must contain a subgroup $\langle a\rangle$ of order 4 but no element of order 8. The subgroup $\langle a\rangle$ is big enough to be normal.

Suppose that G has no other subgroup of order 4. Consider an element b that does not lie in the subgroup generated by a. Then we have (since G is not abelian)

$$a^4 = b^2 = 1, \quad ba = a^3 b.$$

The displayed conditions describe the dihedral group $\boxed{D_4.}$

Otherwise G has a second subgroup $\langle b\rangle$ of order 4. The left cosets of $\langle a\rangle$ are itself and $b\langle a\rangle$, so that $b^2 \in \langle a\rangle$. Thus $a^2 = b^2$. Now we have

$$a^4 = b^4 = 1, \quad a^2 = b^2, \quad ba = a^3 b,$$

and so

$$G = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}.$$

To understand the group better, let

$$c = ab.$$

Then

$$c^2 = ab \cdot ab = a^4 b^2 = b^2 = a^2,$$

so that, since $c^{-1} = b^3 a^3 = ab^3 = a^3 b$,

$$\begin{aligned} ab &= c, & ba &= a^3 b = c^{-1}, \\ bc &= bab = a^3 b^2 = a, & cb &= ab^2 = a^3 = a^{-1}, \\ ca &= aba = b, & ac &= a^2 b = b^3 = b^{-1}. \end{aligned}$$

We see that the G is the group of *Hamiltonian quaternions.*

6. Groups of Order 12

Consider a nonabelian group G of order 12.

Let $K = \{1, a, a^2\}$ be a 3-Sylow subgroup, so that $|G/K| = 4$. The left-translation action of G on the coset space G/K gives a homomorphism

$$\sigma : G \longrightarrow \mathrm{Aut}(G/K) \approx S_4, \quad g \longmapsto (\sigma_g : \gamma K \mapsto g\gamma K).$$

(Note that $\mathrm{Aut}(G/K)$ is a group even though G/K may not be.) The kernel of σ is a subgroup of K since for any g in the kernel we must have $gK = K$.

If σ has trivial kernel then $\boxed{G = A_4.}$ (Recall that A_n is the unique index-2 subgroup of S_n. Indeed, if $H \subset S_n$ doesn't contain some 3-cycle then there are at least three cosets. So an index-2 subgroup contains all 3-cycles, making it A_n.)

Otherwise, the kernel of σ is K, making K a normal subgroup of G. Let Q be a 2-Sylow subgroup of G. Since

$$G = KQ, \quad K \lhd G, \quad K \cap Q = 1_G,$$

G is a semidirect product of K and Q. The only question is how Q acts on the generator a of K by conjugation.

The order-4 group Q is abelian. If its isomorphism type is $C_2 \times C_2$ then it takes the form $Q = \{1, b, c, bc\}$ where $b^2 = c^2 = 1$ and $cb = bc$. In this case, the only nontrivial action of Q on K is, up to relabeling,

$$bab = a, \quad cac = a^2,$$

and so

$$G = \langle a, b, c \,|\, a^3 = b^2 = c^2 = 1,\ ba = ab,\ cb = bc,\ ca = a^2c \rangle.$$

Here the element ab has order 6, and its inverse is a^2b, and its conjugate under the order 2 element c is its inverse,

$$cabc = a^2b.$$

Thus $\boxed{G = D_6.}$

On the other hand, if the isomorphism type of Q is C_4 then $Q = \{1, b, b^2, b^3\}$. In this case, the only nontrivial action of Q on K is $bab^{-1} = a^2$, and so

$$G = \langle a, b \,|\, a^3 = b^4 = 1,\ ba = a^2b \rangle.$$

Alternatively, let $\tilde{a} = ab^2$. Then also

$$G = \langle \tilde{a}, b \,|\, \tilde{a}^6 = 1,\ b^2 = \tilde{a}^3,\ b\tilde{a} = \tilde{a}^5 b \rangle.$$

We don't yet know that such a group exists, but in fact it manifests itself as a subgroup of the cartesian product $S_3 \times C_4$, specifically the subgroup generated by

$$\tilde{a} = ((1\,2\,3), g^2), \quad b = ((1\,2), g), \quad \text{where } g \text{ generates } C_4.$$