II.M. Some results on finite groups

Low order. Let's review what we already know about classifying these. By Lagrange's theorem, if a group has prime order $= p$, then any element $\neq 1_G$ has order p, hence generates the group. So

(II.M.1) (a) groups of prime order are cyclic ($\cong \mathbb{Z}_p$).

This covers orders 2, 3, 5, 7, 11, 13, ... Next,

(b) groups of order $2p$ are either cyclic ($\cong \mathbb{Z}_{2p}$) or dihedral ($\cong D_p$).

This takes care of orders 6, 10, 14, ... Finally,

(c) groups of order p^2 (p prime) are abelian and $\cong \mathbb{Z}_p \times \mathbb{Z}_p$ or $\mathbb{Z}_{p^2}$.

This finishes off orders 4, 9, ... Between 1 and 16 this leaves orders

$$8, \quad 12, \quad \text{and} \quad 15.$$

II.M.2. THEOREM. *The groups of order* 8 *are* (*up to* $\cong$)

$$\mathbb{Z}_8,\ \mathbb{Z}_4 \times \mathbb{Z}_2,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2,\ Q, \text{ and } D_4.$$

PROOF. We begin with the abelian case. By II.L.8 there is a subgroup H of order 4. Any $g \in G \backslash H$, together with H ($\cong \mathbb{Z}_2 \times \mathbb{Z}_2$ or $\mathbb{Z}_4$) generates G.

If $|\langle g \rangle| = 2$, G is $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ or $\mathbb{Z}_2 \times \mathbb{Z}_4$. (Use II.E.11(iv).)

If $|\langle g \rangle| = 8$, $G \cong \mathbb{Z}_8$ (and $H \cong \mathbb{Z}_4$).

If $|\langle g \rangle| = 4$: we need to show that there is an element $g' \in G$ of order 2 and different from $2g$. (Then II.E.11(iv) implies that $G \cong \langle g \rangle \times \langle g' \rangle \cong \mathbb{Z}_4 \times \mathbb{Z}_2$.) Under $G \twoheadrightarrow G/H \cong \mathbb{Z}_2$, we have $g \mapsto \bar{1} \implies 2g \mapsto \bar{0} \implies 2g \in H$ (of order 2). If $H = \langle h \rangle \cong \mathbb{Z}_4$, then $2g = 2h$ and we can take $g' := g - h$. If $H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, then we take g' to be an element of H other than 1 and $2g$.

Turning to the nonabelian case: clearly, we can't have an element of order 8. Also, were every non-identity element of order 2, we'd have

$$1 = (ab)^2 = abab \implies ab = b^{-1}a^{-1} = ba \implies G \text{ abelian.}$$

So there exists an element $a \in G$ of order 4.

Since subgroups of index 2 are normal (cf. II.I.8), $\langle a \rangle \trianglelefteq G$. Pick $b \in G \backslash \langle a \rangle$; then $G = \langle a, b \rangle$, with $b^2 \in \langle a \rangle$. So $b^2 = a^\mu$, where $\mu \neq 1$ or 3 (otherwise $|\langle b \rangle| = 8$); that is,

$$b^2 = a^2 \text{ or } 1. \tag{II.M.3}$$

By the normality, $bab^{-1} \in \langle a \rangle$. Since bab^{-1} has the same order as a, $bab^{-1} = a^{\pm 1}$. But if $bab^{-1} = a$, then b and a commute and G is abelian. So

$$bab^{-1} = a^{-1}, \tag{II.M.4}$$

i.e. $ba = a^{-1}b$.

Now (II.M.3) and (II.M.4) completely describe the multiplication in a group of order 8 with elements $1, a, a^2, a^3, b, ba, ba^2, ba^3$:

$$b^2 = a^2 \text{ or } 1,\ b^{-1} = a^2 b \text{ or } b,\ ab = ba^3,\ a^2 b = ba^2, \text{ etc.}$$

There are two cases: first, if $b^2 = 1$, then we clearly get an isomorphism from $D_4 \overset{\cong}{\to} G$ by sending $r \mapsto a$ and $h \mapsto b$. Second, if $b^2 = a^2$, there is an isomorphism from the quaternions $Q \overset{\cong}{\to} G$ sending $\mathbf{i} \mapsto a$ and $\mathbf{j} \mapsto b$ (and $-1 \mapsto a^2 = b^2$); the reader should check the remaining details. □

Next up would be 12, but this is harder — we'll just list those: D_6, $\mathfrak{A}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_6$, $\mathbb{Z}_{12}$, and the "third[29] dicyclic group"

$$T := \langle a, b \mid a^6 = 1,\ b^2 = a^3 = (ab)^2 \rangle.$$

There is only one group of order 15, namely $\mathbb{Z}_{15}$; this will follow from results below on groups of order pq. But there are *14 non-isomorphic groups of order 16*, so that's a good place to stop this initial mini-foray into group classification.

[29] This is a series of groups of order $4n$: for $n = 1$, $\mathbb{Z}_2 \times \mathbb{Z}_2$; for $n = 2$, Q; for $n = 3$, T; etc.

High(er) order. Here we can really get going with the Sylow theorems, but first we require a few "counting" results. The first is immediate from HW 4 #2:

II.M.5. LEMMA. $H, K \leq G \implies \frac{|H||K|}{|H \cap K|} \leq |G|$.

For $n = \prod_{i=1}^{t} p_i^{e_i}$, recall that

$$\mathrm{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^* \cong \mathbb{Z}_{p_1^{e_1}}^* \times \cdots \times \mathbb{Z}_{p_t^{e_t}}^*$$

has order $\phi(n) := \{k \in \mathbb{Z}_{>0} \mid k < n,\ (k,n) = 1\}$; e.g., $\phi(p) = p-1$, $\phi(p^2) = p(p-1)$, $\phi(p^3) = p^2(p-1)$ etc. for p prime. (One can also prove that $\mathbb{Z}_p^* \cong \mathbb{Z}_{p-1}$ — i.e. it is actually cyclic — which we'll do later on but won't need here.) I will also use without proof

$$\mathrm{Aut}(\underbrace{\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{k \text{ times}}) \cong \mathrm{GL}(k, \mathbb{Z}_p), \tag{II.M.6}$$

where the RHS means $k \times k$ invertible matrices with entries[30] mod p. For $k = 1$, this just says $\mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_p^*$ (with order $p-1$). For $k = 2$ it reads

$$\mathrm{Aut}(\mathbb{Z}_p \times \mathbb{Z}_p) \cong \mathrm{GL}(2, \mathbb{Z}_p)$$

with order $(p-1)^2 p(p+1)$; you will prove this case in the next HW.

We don't actually need much of this for our first result, on groups of order pq:

II.M.7. THEOREM. *Let p and q be distinct primes, with $p > q$ and $q \nmid p-1$. Then the only group of order pq is $\mathbb{Z}_{pq}$.*

PROOF. Let $|G| = pq$ and H, K be the subgroups of order p resp. q guaranteed by Cauchy. By Lagrange's theorem, (i) $H \cap K = \{1\}$; and clearly (ii) $|H||K| = |G|$.

[30] For this to make sense, you need to multiply and add in $\mathbb{Z}_p$, which means to consider it as a *ring*. Since we're about to start that part of the course, it seems fair to mention it! Of course, the automorphisms on the left of (II.M.6) are as an abelian group, and $\mathrm{GL}(k, \mathbb{Z}_p)$ itself is a (nonabelian) mutliplicative group. This generalizes our earlier example $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong \mathfrak{S}_3$ from II.J.4(i) of the group of automorphisms of an abelian group being nonabelian, since $\mathfrak{S}_3 \cong \mathrm{GL}(2, \mathbb{Z}_2)$.

Moreover, we claim that $H \trianglelefteq G$. Otherwise, a *distinct* conjugate H' would be of the same order p, and (again by Lagrange) $H \cap H' = \{1\}$. Lemma II.M.5 then gives $|G| \geq |H||H'| \implies pq \geq p^2 \implies q \geq p$, a contradiction.

Now, consider the composition

$$\text{(II.M.8)} \qquad \mathbb{Z}_q \xrightarrow{\cong} K \xrightarrow{\iota_{(\cdot)}} \mathrm{Aut}(H) \xrightarrow{\cong} \mathrm{Aut}(\mathbb{Z}_p) \xrightarrow{\cong} \mathbb{Z}_p^* \qquad (\mu)$$

induced by conjugating elements of H by elements of K (since $H \trianglelefteq G$). By the Fundamental Theorem,

$$|\mathrm{im}(\mu)| \big| |\mathbb{Z}_p^*|, |\mathbb{Z}_q|.$$

If $q \nmid p-1$, this is impossible unless $|\mathrm{im}(\mu)| = 1$. Hence, the map (II.M.8) is trivial, and $\iota_k = \mathrm{id}_H$ ($\forall k \in K$); i.e. $khk^{-1} = h$ ($\forall h \in H, k \in K$) or (iii) $kh = hk$ ($\forall h, k$).

The three hypothesis (i),(ii),(iii) imply (by the Direct Product Theorem II.E.11(iv)) that $G \cong H \times K \cong \mathbb{Z}_p \times \mathbb{Z}_q$, which is $\cong \mathbb{Z}_{pq}$ since $(p,q) = 1$. □

Here is another instance of this type of argument:

II.M.9. EXAMPLE. We classify the groups G of order $5^2 \cdot 37^2$. First, there exist

- a Sylow 37-subgroup H (of order 37^2), and
- a Sylow 5-subgroup K (of order 5^2).

Clearly $|H||K| = |G|$, and $H \cap K = \{1\}$.

Moreover, $H \trianglelefteq G$: if it had a distinct conjugate H', then $|H \cap H'|$ is either 37 or 1, so that

$$5^2 \cdot 37^2 = |G| \geq \frac{|H||H'|}{|H \cap H'|} = \frac{37^2 \cdot 37^2}{37 \text{ or } 1} = 37^3 \text{ or } 37^4$$

yields a contradiction.

Thus K acts on H by conjugation, yielding a homomorphism

$$\varphi \colon K \to \mathrm{Aut}(H).$$

Being a group of order p^2, $p = 37$ prime, H is one of the following (cf. II.H.9):

- $H \cong \mathbb{Z}_{p^2} \implies \mathrm{Aut}(H) \cong \mathbb{Z}_{p^2}^*$ has order $p(p-1) = 37 \cdot 36$; or
- $H \cong \mathbb{Z}_p \times \mathbb{Z}_p \implies \mathrm{Aut}(H) \cong \mathrm{GL}(2, \mathbb{Z}_p)$ has order $p(p+1)(p-1)^2 = 37 \cdot 38(36)^2$.

But for φ to be compatible with the Fundamental Theorem, we must have $|\mathrm{im}(\varphi)| \big| |K|, |\mathrm{Aut}(H)|$; and 25 is relatively prime to 37, 36, and 38. We conclude that $\mathrm{im}(\varphi) = \{1_{\mathrm{Aut}(H)}\}$, so that $kh = hk$ $(\forall k, h)$ as in the last proof. Once again, $G \cong H \times K$ which yields the four possibilities:

- $G \cong \mathbb{Z}_{37^2} \times \mathbb{Z}_{5^2} \cong \mathbb{Z}_{5^2 37^2}$;
- $G \cong (\mathbb{Z}_{37} \times \mathbb{Z}_{37}) \times \mathbb{Z}_{5^2} \cong \mathbb{Z}_{37} \times \mathbb{Z}_{37 \cdot 5^2}$;
- $G \cong \mathbb{Z}_{37^2} \times (\mathbb{Z}_5 \times \mathbb{Z}_5) \cong \mathbb{Z}_{37^2 \cdot 5} \times \mathbb{Z}_5$; and
- $G \cong (\mathbb{Z}_{37} \times \mathbb{Z}_{37}) \times (\mathbb{Z}_5 \times \mathbb{Z}_5) \cong \mathbb{Z}_{5 \cdot 37} \times \mathbb{Z}_{5 \cdot 37}$.

In particular, G is abelian!

Recall that $\mathfrak{A}_5$ was a simple group, i.e. had no normal subgroups apart from itself and $\{1\}$. Also, $|\mathfrak{A}_5| = \frac{5!}{2} = 60$. Here is a beautiful application of Sylow theory which attests to the "specialness" of $\mathfrak{A}_5$.

II.M.10. THEOREM. *There is no nonabelian simple group of order less than* 60.

PROOF. We know that

- groups of prime order are simple but abelian, and
- groups of prime power order are *not* simple (cf. II.L.8).

Suppose that there exists a nonabelian group G, simple of order

$$|G| = p^e m,\ m > 1,\ p \text{ prime},\ p \nmid m,\ p^e \nmid (m-1)!. \tag{II.M.11}$$

By Sylow I, G has a subgroup H of order p^e and index m. Letting G act on left cosets G/H by left-multiplication gives a homomorphism $\varphi\colon G \to \mathfrak{S}_m$ which must be injective or trivial (so that $\ker(\varphi)$ doesn't furnish a normal subgroup other than $\{1\}$ or G). In fact, it can't be trivial, as G acts transitively on H's cosets. So φ is injective, and

$\varphi(G) \leq \mathfrak{S}_m$ has order $p^e m$. By Lagrange, $p^e m | m! \implies p^e \mid (m-1)!$ in contradiction to our assumption.

Now the only positive integers less than 60 and not of the form (II.M.11), and not a prime or prime power, are 30, 40, and 56. We shall systematically rule these out as possible orders of simple groups.

Suppose $|G| = 30 = 2 \cdot 3 \cdot 5$, and take P to be a Sylow 5-subgroup. By Sylow II, the number of conjugates of P satisfies $N_P \underset{(5)}{\equiv} 1$; while by (II.L.10) $N_P \mid 30$. Moreover, if G is to be simple, then P can't be normal, so $N_P > 1$; and we deduce that $N_P = 6$. Next, a 3-Sylow subgroup Q has $N_Q \underset{(3)}{\equiv} 1$, $N_Q | 30$, and $N_Q \neq 1$, hence $N_Q = 10$. By Lagrange, none of the six conjugates of P and 10 conjugates of Q can intersect outside of $\{1\}$. This requires G to have at least

$$(5-1) \cdot 6 + (3-1) \cdot 10 + 1 = 45 \text{ elements},$$

which, well, it doesn't.

How about $|G| = 40 = 2^3 \cdot 5$? Let P be a Sylow 5-subgroup. If N is its number of conjugates, then $N \underset{(5)}{\equiv} 1$, $N \neq 1$, and $N \mid 40$. There's no such number N.

Finally, there's $|G| = 56 = 2^3 \cdot 7$ to take out. Write P for a Sylow 7-subgroup, with N_7 conjugates. We have $N_7 \underset{(7)}{\equiv} 1$, $N_7 \neq 1$, and $N_7 \mid 56$ $\implies N_7 = 8$. Playing the same game with a Sylow 2-subgroup Q gives $N_2 \geq 3$ conjugates. Now the conjugates of P can't intersect each other or those of Q outside of the identity element; not counting the identity, this furnishes $N_7 \cdot (7-1) = 8 \cdot 6 = 48$ distinct elements of G. On the other hand, the conjugates of Q (which, remember, have order 8) *can* intersect in order-4 subgroups. Without thinking too hard, we at least get (counting the identity) 12 additional elements of G by considering just Q and one conjugate. This again produces a contradiction since $12 + 48 = 60 > 56$, concluding the proof. □

Miscellany. Before we leave the realm of finite group classification, I would be remiss not to mention the famous *classification of all finite simple groups* (completed in 2004) into:

- cyclic groups of prime order $\mathbb{Z}_p$
- alternating groups $\mathfrak{A}_n$, $n \geq 5$ (Galois, 1832)
- simple groups of Lie type:
  - This starts from É. Cartan's classification (1894) of complex simple Lie algebras into the *Cartan types* A_n ($\mathfrak{sl}_{n+1}$), B_n ($\mathfrak{so}_{2n+1}$), C_n ($\mathfrak{sp}_{2n}$), D_n ($\mathfrak{so}_{2n}$), G_2, F_4, E_6, E_7, E_8.
  - C. Chevalley (1955) constructed integral bases for these, allowing him to define the corresponding simple Lie groups as algebraic groups over the integers, hence also over finite fields (e.g. $\mathbb{Z}_p$, by reducing modulo p).
  - e.g. $\mathrm{PSL}_m(\mathbb{Z}_p)$ is obvious; not so with $G_2(\mathbb{Z}_p)$.
  - Steinberg, Suzuki, Ree filled in gaps (e.g. unitary groups).
- 26 sporadic simple groups
  - the "Monster" is the largest, of order $\simeq 8 \times 10^{53}$
  - Mathieu groups are the most approachable, as automorphism groups of "Steiner systems": e.g., $S(4,5,11)$ denotes a set $\mathscr{P}$ of 11 points, together with a set $\mathscr{B}$ of "blocks" of 5 points each, such that each 4-point subset of $\mathscr{P}$ belongs to a unique block; and $M_{11} \leq \mathfrak{S}_{\mathscr{P}} \cong \mathfrak{S}_{11}$ is the subgroup preserving blocks.

Another two topics oddly missing from [**Jacobson**] are group extensions and semidirect products. They deserve a brief mention now, as interesting constructions of (non-simple) finite groups.

We start with group extensions (of a group H by a group K). These are **short-exact sequences** of groups

$$\varepsilon := \{1 \to K \xrightarrow{\alpha} G \xrightarrow{\beta} H \to 1\}. \tag{II.M.12}$$

That is, α is an injective homomorphism, β is a surjective homomorphism, and $\ker(\beta) = \mathrm{im}(\alpha)$. Hence,[31] $H \cong G/\alpha(K)$ and $\alpha(K) \trianglelefteq G$.

[31]Note that since α is injective, $\alpha(K) \cong K$. The "1" on each end of the sequence is a formality, which can be read as saying the kernel of α is the image of "1" (i.e. trivial), and the image of β is the kernel of $H \to 1$ (i.e. all of H).

II.M.13. EXAMPLE. The n^{th} **dicyclic group**

$$\mathrm{Dic}_n := \langle a, b \mid a^{2n} = 1,\ b^2 = a^n,\ b^{-1}ab = a^{-1} \rangle$$

sits in a short-exact sequence

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathbb{Z}_{2n} & \longrightarrow & \mathrm{Dic}_n & \longrightarrow & \mathbb{Z}_2 & \longrightarrow & 1\ . \\ & & & & b & \longmapsto & \bar{1} & & \\ & & \bar{1} & \longmapsto & a & \longmapsto & \bar{0} & & \end{array}$$

Referring to (II.M.12), one says that

$$\varepsilon \textbf{ splits} \iff \exists \text{ homomorphism } \gamma\colon H \to G \text{ with } \beta\gamma = \mathrm{id}_H.$$

This displays $H \cong \gamma(H)$ as a (not necessarily normal) subgroup of G, since such a homomorphism is necessarily injective (why?). One easy example: $G = H \times K$ is a split extension of H by K. Here is another:

II.M.14. EXAMPLE. Recall the presentation

$$D_n = \langle a, b \mid a^n = 1,\ b^2 = 1,\ b^{-1}ab = a^{-1} \rangle$$

of the n^{th} dihedral group. We have

$$\begin{array}{ccccccccc} & & & & b & \overset{\gamma}{\longmapsto} & \bar{1} & & \\ 1 & \longrightarrow & \mathbb{Z}_n & \longrightarrow & D_n & \longrightarrow & \mathbb{Z}_2 & \longrightarrow & 1 \\ & & & & b & \overset{\beta}{\longmapsto} & \bar{1} & & \\ & & \bar{1} & \longmapsto & a & \longmapsto & \bar{0} & & \end{array}$$

so in this case the extension is split: γ yields a homomorphism because $1_{D_n} = \gamma(\bar{0}) = \gamma(\bar{1} + \bar{1}) = \gamma(\bar{1})^2 = y^2$ does indeed hold. (This won't work in example II.M.13 since there's no element of order 2 in $\beta^{-1}(\bar{1}) \subset \mathrm{Dic}_n$.)

So split extensions are more general than direct products, though they are nicer than general group extensions. Can we characterize them in some useful way?

II.M.15. DEFINITION. Let $\theta\colon H \to \mathrm{Aut}(K)$ be a homomorphism, sending $h \mapsto \theta_h$. The **semidirect product** $K \rtimes_\theta H$ is the group with

underlying set $K \times H$ and product

$$(k, h) \cdot (k', h') := (k \cdot \theta_h(k'), h \cdot h').$$

II.M.16. PROPOSITION. *The extension $\boldsymbol{\varepsilon}$ splits $\iff$ G is a semidirect product of K and H.*

PROOF. ($\implies$): Write $H = \gamma(H)$ and $K = \alpha(K)$ as subgroups of G. Define $\theta\colon H \to \mathrm{Aut}(K)$ by $h \mapsto \imath_h$; this works since $K \trianglelefteq G$. (That is, $\theta_h := \imath_h$ is conjugation by h.) As $H \cong G/K$, the map *of sets* $\mu\colon K \times H \to G$ sending $(k, h) \mapsto kh$ is bijective. Now compute:

$$\begin{aligned}\mu(k, h)\mu(k', h') &= khk'h' = khk'h^{-1}hh' \\ &= \mu(k\theta_h(k'), hh').\end{aligned}$$

The reverse direction ($\impliedby$) is HW. □

II.M.17. EXAMPLE. The *mod 3 Heisenberg group* consists of matrices

$$\begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ c & b & 1 \end{pmatrix}$$

with entries mod 3 (i.e. in $\mathbb{Z}_3$). While non-abelian, it has the same number of elements of each order as $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$. There is a natural way to write this as an extension of $\mathbb{Z}_3 \times \mathbb{Z}_3$ by $\mathbb{Z}_3$. Does it split? (This is a useful question to ask when looking at HW 5 #1.)