3. Group theory

3.1. **The basic isomorphism theorems.** If $f : X \to Y$ is any map, then $x \sim x'$ if and only if $f(x) = f(x')$ defines an equivalence relation on X. Recall that the quotient $\overline{X} = X/\sim$ was defined as the set of equivalence classes $\overline{X} = \{\overline{x} : x \in X\}$, $\overline{x} = \{y \in X : y \sim x\}$. We can now *factor* the map f by going through $\overline{X}$: we have that $f = \overline{f} \circ q$, where $q : X \to \overline{X}$ is the natural map $q(x) = \overline{x}$, and $\overline{f}(\overline{x}) = f(x)$.

Exercise 3.1. Check that $\overline{f}$ is well defined and injective, and q is surjective.

This is really an extremely simple construction: we first lump together those points of X that get sent to the same image by f, and then we apply f. It sometimes helps the intuition to represent this diagrammatically, as follows:

(3.1)
$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle q}\downarrow & \nearrow_{\overline{f}} & \\ \overline{X} & & \end{array}$$

We say that a diagram *commutes* to express the fact that no matter how you follow arrows to get from A to B, the resulting map will be the same. Diagram (3.1) is commutative: the only journey where we have a choice is the one from X to Y, so this says that $f = \overline{f} \circ q$, which we observed above.

One can pack even more information into these diagrams by using special arrows for specific types of maps. Then the above diagram becomes

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle q}\downarrow\!\!\downarrow & \nearrow_{\overline{f}} & \\ \overline{X} & & \end{array} .$$

This indicates that q is surjective and $\overline{f}$ is injective. Another property of this diagram (and the original construction) is that (of course) $\overline{f}$ is the *only* map between $\overline{X}$ and Y that will give us the identity $f = \overline{f} \circ q$ or, equivalently, that will make the diagram commute. One can use a dashed arrow to emphasize that there exists a unique map:

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle q}\downarrow\!\!\downarrow & \nearrow_{\overline{f}} & \\ \overline{X} & & \end{array} .$$

Of course, we can do the same thing for a homomorphism $\varphi : G \to G'$ between groups. In this case, the maps $q, \overline{f}$ will then be homomorphisms themselves.

Theorem 3.1. *Let $\varphi : G \to G'$ be a homomorphism. Then $K = \ker(\varphi)$ is a normal subgroup of G, the quotient map $q : G \to G/K$, $q(a) = aK$ is a surjective homomorphism, and there exists a unique map $\overline{\varphi} : G/K \to G'$ that makes the following diagram commute:*

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G' \\ {\scriptstyle q}\downarrow & \nearrow_{\overline{\varphi}} & \\ G/K & & \end{array} .$$

This map $\overline{\varphi}$ is an injective homomorphism, and $\varphi(G) \cong G/K$.

This is sometimes and somewhat grandiosely called the *fundamental theorem of homomorphisms.*

Proof. We know most of this already, and the remaining statements are established by checking them against the definitions. $K \trianglelefteq G$ by Proposition 2.24, and we also saw earlier (show it again perhaps) that the natural map $q : G \to G/K$, $q(a) = aK$, is a surjective homomorphism. Next, observe that $q(a) = q(b)$ precisely if $\varphi(a) = \varphi(b)$ (show that too more explicitly if you are not sure), so we *are* running the same construction as above, only for groups and homomorphisms rather than general sets and maps. We obtain a unique, injective map $\overline{\varphi} : G/K \to G'$ that makes the diagram commutative; it is given by $\overline{\varphi}(aK) = \varphi(a)$. So

$$\overline{\varphi}(aKbK) = \varphi(ab) = \varphi(a)\varphi(b) = \overline{\varphi}(aK)\overline{\varphi}(bK),$$

and this says that $\overline{\varphi}$ is a homomorphism, as claimed. The image of $\overline{\varphi}$ is $\varphi(G)$, so since $\overline{\varphi}$ is injective, it is an isomorphism between G/K and this group. □

Exercise 3.2. Formulate and prove a version of Theorem 3.1 for monoids. Remember that there is no analog of the correspondence between congruences and normal subgroups, so you will have to work with congruences here.

Corollary 3.2. *A group G' is a homomorphic image of the group G precisely if $G' \cong G/K$ for some $K \trianglelefteq G$.*

Proof. If $G' = \varphi(G)$, then $G' \cong G/K$ is part of what Theorem 3.1 gives. Conversely, if φ maps G/K isomorphically onto G', then $\varphi \circ q$, with $q : G \to G/K$ being the quotient map, is a homomorphism from G onto G'. □

Exercise 3.3. The last part of this argument uses the fact that a composition of homomorphisms is a homomorphism itself. Prove this please.

Exercise 3.4. Let G be a finite group, and let $\varphi : G \to G'$ be a homomorphism. Show that $|\varphi(G)|$ divides $|G|$.

Exercise 3.5. (a) Find a non-trivial (that is, $\varphi(a) \neq 1$ for some a) homomorphism $\varphi : S_3 \to \mathbb{Z}_2$ (there is exactly one such φ, and we discussed it earlier, in slightly different form).
(b) Show that there is no non-trivial homomorphism $\varphi : S_3 \to \mathbb{Z}_3$.

A somewhat more general form of Theorem 3.1 is sometimes useful, for example in the proof of the first isomorphism theorem below.

Theorem 3.3. *Let $K \trianglelefteq G$, and let $\varphi : G \to G'$ be a homomorphism with $\ker(\varphi) \supseteq K$. Then there exists a unique map $\overline{\varphi}$ such that the following diagram commutes:*

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G' \\ {\scriptstyle q}\downarrow & \nearrow_{\overline{\varphi}} & \\ G/K & & \end{array}$$

This map is a homomorphism with $\ker(\overline{\varphi}) = \ker(\varphi)/K = \{aK : a \in \ker(\varphi)\}$.

Theorem 3.1 is the special case $K = \ker(\varphi)$; note that in this case,

$$\ker(\overline{\varphi}) = \ker(\varphi)/K = K/K = \{K\} = \{\overline{1}\} \subseteq G/K,$$

so $\overline{\varphi}$ is now injective, as already observed above.

Exercise 3.6. Prove Theorem 3.3 in the same style as above, by checking directly the various claims. Pay special attention to the role of the assumption that $K \subseteq \ker(\varphi)$; what goes wrong if we don't have this?

Theorem 3.4 (First isomorphism theorem)**.** *Let $K \trianglelefteq G$. Then the subgroups H of G with $H \supseteq K$ are in one-to-one correspondence with the subgroups of $\overline{G} = G/K$ via $H \mapsto H/K = \{hK : h \in H\} =: \overline{H}$.*

Moreover, for such a subgroup $K \subseteq H \subseteq G$, we have that $H \trianglelefteq G$ if and only if $\overline{H} \trianglelefteq \overline{G}$. In this case, $\overline{G}/\overline{H} \cong G/H$, and an isomorphism φ may be obtained from the diagram

$$\begin{array}{ccc} G & \xrightarrow{q} & G/K \\ {\scriptstyle p}\downarrow & \swarrow & \downarrow{\scriptstyle r} \\ G/H & \xleftarrow{\varphi} & \overline{G}/\overline{H} \end{array};$$

here p, q, r are the natural quotient maps.

It is tempting to view this isomorphism as the result of a cancellation $(G/K)/(H/K) \cong G/H$, but one must be very careful with such formal manipulations (for starters, multiplication is not commutative in groups), and we will see in a moment that, for example, HK/K is not isomorphic to H in general.

Proof. Clearly, if $H \supseteq K$ is any subgroup of G, then K is normal in H since it was normal in the larger group G. So we can form the quotient group H/K, and this is a subgroup of G/K. To show that this map $H \mapsto H/K$ is injective, suppose that $H_1/K = H_2/K$ and take any $h_1 \in H_1$. Then $h_1K \in H_1/K = H_2/K$, so $h_1K = h_2K$ for some $h_2 \in H_2$ and thus $h_2^{-1}h_1 \in K$. Since $K \subseteq H_2$, this shows that $h_1 \in H_2$, so we have shown that $H_1 \subseteq H_2$. Thus $H_1 = H_2$, by symmetry.

To show that the map $H \mapsto H/K$ is surjective onto the subgroups of G/K, let $L \subseteq G/K$ be such a subgroup. So L is a collection of certain cosets aK, and let's now define $H \subseteq G$ as the set of those $h \in G$ for which $hK \in L$. Then clearly $K \subseteq H \subseteq G$, and I claim that H is a subgroup of G. Indeed, let $a, b \in H$. Then $aK, bK \in L$, so $ab^{-1}K \in L$ as well, and thus $ab^{-1} \in H$, as desired. By construction, $H/K = L$.

Notice that $H/K \trianglelefteq G/K$ precisely if $(aK)(hK)(aK)^{-1} \in H/K$ for all $h \in H, a \in G$, but this is the same as asking that $aha^{-1}K \in H/K$, and this happens if and only if $aha^{-1} \in H$. Here, we use the description of H that was obtained in the preceding paragraph: H is the collection of all $b \in G$ with $bK \in H/K$. It now follows that H is normal in G precisely if $\overline{H}$ is normal in $\overline{G}$.

It remains to show that $G/H \cong \overline{G}/\overline{H}$ if indeed $H \trianglelefteq G$. This will pretty much just fall into place, by making use of the obvious maps between the various quotients. Basically, we can do this by staring at the diagram long enough. We first observe that Theorem 3.3 applies to the upper left half of the diagram, with the quotient map p taking the role of φ from Theorem 3.3. Indeed, since $\ker(p) = H \supseteq K$, we can factor p through q and we obtain an induced map along the dotted diagonal. This map (let's call it θ) is a homomorphism with $\ker(\theta) = \ker(p)/K = H/K = \overline{H}$. Next, we apply Theorem 3.3 to the lower right half of the diagram, with θ taking the role of φ. This time, the kernel of this map θ is exactly what we are dividing out, so we are actually back in the situation of Theorem 3.1. In particular, it follows that the induced map along the bottom arrow is an *injective* homomorphism. Since θ was surjective, it is surjective also, so it is the required isomorphism. Uniqueness is also clear because at each of these two steps, there was only one way to fill up the diagram. $\square$

Theorem 3.5 (Second isomorphism theorem)**.** *Suppose that $K \trianglelefteq G$, and H is a subgroup of G. Then HK and $H \cap K$ are subgroups of G, $K \trianglelefteq HK$, $H \cap K \trianglelefteq H$ and $HK/K \cong H/(H \cap K)$.*

More specifically, an isomorphism can be obtained from

$$\begin{array}{ccc} H & \xrightarrow{\quad q \quad} & H/(H \cap K)\ ; \\ {\scriptstyle \iota}\downarrow & \cdots\searrow & \downarrow{\scriptstyle \varphi} \\ HK & \xrightarrow[\quad p \quad]{} & HK/K \end{array}$$

here, p, q are the natural quotient maps, and ι is the inclusion $\iota(a) = a$, $a \in H$.

Exercise 3.7. Prove this in the same style as Theorem 3.4. More explicitly, proceed as follows: (a) Show that HK is a subgroup and that $K \trianglelefteq HK$, $H \cap K \trianglelefteq H$, by direct verification; (b) construct an isomorphism between $H/(H \cap K)$ and HK/K by working out what the diagram delivers; in a first step, obtain a (unique) map along the dotted diagonal by composing.

Exercise 3.8. Let H, K be two (not necessarily normal) subgroups of a group G. Show that HK need not be a subgroup.

It is instructive to take another look at cyclic groups from the more abstract point of view suggested by the material of this section. (I'll just sketch the relevant steps.) So let $G = \langle a \rangle$ be a cyclic group. Then, as we saw, $\varphi : \mathbb{Z} \to G$, $\varphi(n) = a^n$ defines a surjective homomorphism. Thus $G \cong \mathbb{Z}/K$, where $K = \ker(\varphi)$ is a normal subgroup of $\mathbb{Z}$. Since $\mathbb{Z}$ is abelian, all subgroups are normal. We also saw earlier that these subgroups are given by $K = k\mathbb{Z} = \{kn : n \in \mathbb{Z}\}$. Thus, up to isomorphism, the complete list of cyclic groups is given by $\mathbb{Z}$ and $\mathbb{Z}/k\mathbb{Z}$, $k \geq 1$, and of course $\mathbb{Z}/k\mathbb{Z} \cong \mathbb{Z}_k$, so we have recovered Theorem 2.10.

We now also find the subgroups of cyclic groups from the first isomorphism theorem: the subgroups of $G = \mathbb{Z}_k = \mathbb{Z}/k\mathbb{Z}$ are in one-to-one correspondence to those subgroups of $\mathbb{Z}$ that contain $k\mathbb{Z}$. These are given by $m\mathbb{Z}$ with $m|k$, say $k = rm$, and the corresponding subgroup of G is $m\mathbb{Z}/k\mathbb{Z} \cong \mathbb{Z}_r$, so we also recover the result that there is exactly one subgroup for each divisor of k.

3.2. **Free groups.** We saw in the previous section that not any group G' can be a homomorphic image $G' = \varphi(G)$ of a given group G. Of course, there is the obvious restriction that G' must not be too large set theoretically (you won't be able to map a group with 5 elements, say, onto a group with 5353 elements), but there is more to it than that:

all identities that hold in G will be preserved by φ, so must hold in G' as well. As a concrete very simple illustration, consider for example an abelian group G: this cannot be mapped homomorphically onto a non-abelian group G' because $ab = ba$ in G, and these identities (or *relations,* as we will call them in this context) carry over to the image, so we also must have that $xy = yx$ for any two elements $x = \varphi(a)$, $y = \varphi(b)$ of $\varphi(G)$.

Indeed, we found that the possible homomorphic images of G, up to isomorphism, are exactly the quotient groups G/K, which is consistent with the interpretation just suggested that a possible image is a group that has at least the same relations as G, and maybe additional ones.

It is therefore interesting to try to build groups with as few relations as possible. We would then expect these to have the property that they can be mapped onto anything that isn't simply too large. To make this more precise, we fix a set X of prospective generators, and we would like to construct a group $G = \langle X\rangle$ that does not have any unnecessary relations.

As a warm-up, let's discuss the easier monoid version of this question. The monoid $M = FM(X)$ we are looking for should contain X, so whenever $x_1, \dots, x_n \in X$, then the product $x_1x_2\cdots x_n$, whatever it will turn out to be equal to, must also be in $FM(X)$. We also want $FM(X)$ to be generated by X, as a monoid, so these products of generators should actually be all of $FM(X)$. Finally, since we don't want relations, we will treat any two such products as distinct unless they are identical. We can make these straightforward but somewhat informal remarks precise as follows:

Definition 3.6. Let X be a set. The *free monoid* generated by X is given by the set of words in letters drawn from X,

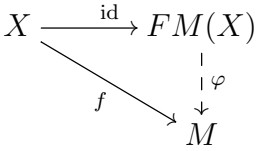
$$FM(X) = \{x_1x_2\dots x_n : n \geq 0, x_j \in X\},$$

with concatenation as the monoid operation and the empty word as the neutral element.

It is straightforward to check (do it please) that $FM(X)$ is indeed a monoid that is generated by X. Moreover, by our introductory remarks, we expect to be able to map $FM(X)$ onto any monoid that isn't too large. This works; here is a slightly more general version of this property:

Theorem 3.7. *Let X be a set and let M be a monoid. Then, given any map $f : X \to M$, there exists a unique homomorphism $\varphi : FM(X) \to M$ such that $f = \varphi \circ \mathrm{id}$, where $\mathrm{id}(x) = x$ (interpreted as a one letter*

word).



Please don't get confused by the dashed arrow φ: the claim is that there exists a unique *homomorphism* that makes the diagram commute (not an arbitrary map).

Proof. Any such φ must clearly satisfy $\varphi(x) = f(x)$ for $x \in X$. This already establishes uniqueness, by Proposition 3.8 below. For general $y = x_1 \dots x_n \in M$, since we want a homomorphism, we are forced to define $\varphi(y) = \varphi(x_1) \dots \varphi(x_n)$, and if $n = 0$, then we are dealing with the neutral element, so φ must send this to $1 \in M$. Having done this, it is now clear that it works. □

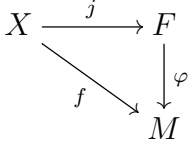
Proposition 3.8. *Let M, M' be monoids, and suppose that M is generated by X. If $\varphi_j : M \to M'$, $j = 1, 2$ are homomorphisms with $\varphi_1(x) = \varphi_2(x)$ for all $x \in X$, then $\varphi_1(y) = \varphi_2(y)$ for all $y \in M$.*

An analogous result holds for groups.

Proof. Let $M_0 = \{y \in M : \varphi_1(y) = \varphi_2(y)\}$ and observe that M_0 is a submonoid of M that contains X, hence $M_0 = M$. The proof for groups is identical. □

We can't make any claims about φ mapping *onto* M in the generality of Theorem 3.7, so we must specialize this if we want a statement of the type announced above. So suppose now that the monoid M is generated by $X \subseteq M$; then we can take f as the inclusion map $f(x) = x$, and we obtain a unique homomorphism $\varphi : FM(X) \to M$ with $\varphi(x) = x$ for $x \in X$. This time, φ will be surjective (why?), so $M = \varphi(FM(X))$. The free monoid with generator set X can be mapped homomorphically onto *any* monoid generated by X, as promised.

Exercise 3.9. Show that $FM(X)$ is actually characterized by these properties, up to isomorphism. More precisely, let $j : X \to F$ be a mapping from a set X to a monoid F, and suppose that if $f : X \to M$ is any map from X to an arbitrary monoid M, then there exists a unique homomorphism φ so that the following diagram commutes:



Show that then $F \cong FM(X)$.

After this warm-up, back to the group case. We want to implement the same strategy. In groups, we can also take inverses, so the *free group* should now contain words in the generators *and their inverses.* This is best handled by temporarily making those inverses independent generators. So given a set X, we introduce the new symbols $X' = \{x' : x \in X\}$, and we then form words

$$a = a_1 a_2 \dots a_n, \qquad n \geq 0, \quad a_j \in X \cup X'$$

with letters taken from $X \cup X'$. Our intention is to eventually recognize the $x' \in X'$ as the inverses $x' = x^{-1}$, $x \in X$. In particular, this time we will have to introduce some relations on our words: whenever an $x \in X$ is immediately followed by the corresponding symbol $x' \in X'$ or vice versa, we may remove both symbols from our word. (It may seem silly to have put these letters xx' there in the first place, but recall that we multiply words by concatenating them, so such pairs can arise unintentionally, at the gluing point.) This is called a *basic reduction;* we write $a \xrightarrow{1} b$ if b is obtained from a by one such reduction step. More formally, $a \xrightarrow{1} b$ means that $b = a_1 a_2 \dots a_{k-1} a_{k+2} \dots a_n$ for some $0 \leq k \leq n-1$ and $a_{k+1} = a_k'$ or $a_k = a_{k+1}'$.

A word a is called *reduced* if no reduction is possible, that is, there is no word b with $a \xrightarrow{1} b$. We will then define $FG(X)$ as the set of all reduced words, with concatenation plus reduction as the group operation. It is intuitively clear that this is the right thing to do and will work, but we'll give a careful formal treatment, too.

We write $a \xrightarrow{n} b$ if b can be obtained from a by precisely n reduction steps, and $a \to b$ means that $a \xrightarrow{n} b$ for some $n \geq 0$; here, we of course interpret $a \xrightarrow{0} b$ as $a = b$.

Exercise 3.10. In this exercise, we will identify binary relations R on a set X with the corresponding subsets $\{(x, y) : x, y \in X, xRy\}$ of $X \times X$.
(a) Given a binary relation R on a set X, show that there is a smallest (as a subset of $X \times X$) *reflexive* relation R_0 with $R_0 \supseteq R$. (This should be easy; give a direct definition of R_0.)
(b) Next, show that there is a smallest *transitive* relation R_t with $R_t \supseteq R_0$. This is called the *transitive closure* of R_0. (This isn't very difficult either, but perhaps an abstract argument will work best.)
(c) Show that $\to$ is the transitive closure of the reflexive version $(\xrightarrow{1})_0$ of $\xrightarrow{1}$.

It is clear that any word a can be reduced to a reduced word, that is, there exists a reduced word b with $a \to b$. Indeed, all we need to do is

reduce a as long as this is still possible; since each individual reduction step decreases the length of a by 2 digits, the process must stop after finitely many steps. However, when reducing a given word a in this way, we may have to make choices, so the reduction process itself is certainly not uniquely determined by a. For example, if $a = xx'xy'y$, then there are three possible reductions $a \xrightarrow{1} b$ in the first step already.

The following property of reductions will be crucial in the construction of the free group:

Lemma 3.9. *For every word $a \in FM(X \cup X')$, there is a* unique *reduced word b such that $a \to b$.*

So while the journey from a to b is not unique, the final destination is. This is sometimes expressed by saying that reduction $\to$ is a *confluent* relation.

If you try some examples (such as the word $a = xx'xy'y$ from above), you will quickly become convinced that Lemma 3.9 is true. A clean formal proof still requires some care, though. Let's first look at a very basic case.

Lemma 3.10. *If $a \xrightarrow{1} b$ and $a \xrightarrow{1} c$ and $c \neq b$, then $b \xrightarrow{1} d$, $c \xrightarrow{1} d$ for some d.*

Proof. Let's say we get from a to b by deleting $a_k a_{k+1}$ (so $a_{k+1} = a'_k$ or the other way around), and we obtain c by deleting $a_j a_{j+1}$ from a. Now if these pairs don't overlap, then the claim is clear: we simply delete $a_j a_{j+1}$ from b and $a_k a_{k+1}$ from c to get to d.

But this is actually the general case: we certainly can't have $k = j$ because this would give $b = c$, contrary to our assumption. If $j = k+1$, say, then we still arrive at the same conclusion $b = c$: this time, a contains a piece of the form $xx'x$ (or $x'xx'$), and whether we delete xx' or $x'x$, the net effect is the same. □

We are now ready for the

Proof of Lemma 3.9. We will show that if $a \to b$, $a \to c$, then there is a d such that $b \to d$, $c \to d$. This will give the Lemma because it in particular says that if b, c are *reduced* words here, then only the trivial reduction to $d = b = c$ is possible, so $b = c$.

We are, more specifically, assuming that $a \xrightarrow{j} b$, $a \xrightarrow{k} c$, and we will prove our claim by a double induction on j, k. Everything becomes trivial if $j = 0$ or $k = 0$. So let's for now focus on the case $k = 1$. As announced, we will proceed by induction on j. If $j = 1$ (= basis of the induction), then we're back in the situation of Lemma 3.10. Now let (= inductive step) $j \geq 2$ and suppose that what we're currently

trying to show holds for $j-1$. In other words, if $a \xrightarrow{j-1} b$, $a \xrightarrow{1} c$, then b, c can both be reduced to a common word d. Now suppose that $a \xrightarrow{j} b$ and $a \xrightarrow{1} c$. We can split off the first step in the first reduction, say $a \xrightarrow{1} u \xrightarrow{j-1} b$. If $u = c$ here, then we can take $d = b$ and we're done (with this part). If not, then Lemma 3.10 applies to the one-step reductions $a \xrightarrow{1} u$, $a \xrightarrow{1} c$, and we obtain a word v with $u \xrightarrow{1} v$, $c \xrightarrow{1} v$. Now the induction hypothesis, applied to $u \xrightarrow{j-1} b$, $u \xrightarrow{1} v$, produces a d with $b \to d$, $v \to d$, and this d is then also a common reduction of b, c, as required. We have established the claim for $k = 1$ and arbitrary j.

Now we finish with a final induction on k. We just discussed the case $k = 1$. Let $k \geq 2$, and assume the claim for $k-1$. Suppose that $a \xrightarrow{j} b$ and $a \xrightarrow{1} u \xrightarrow{k-1} c$. Since we can now handle the $k = 1$ case, we obtain that $b \to v$, $u \to v$ for some v. Now the induction hypothesis can be applied to $u \xrightarrow{n} v$, $u \xrightarrow{k-1} c$, and we find that v, c reduce to a common word d, and thus $b \to d$, $c \to d$ as well. □

We are now ready to give a preliminary definition of the *free group* with generator set X. Notice that given a word $a \in FM(X \cup X')$, Lemma 3.9 allows us to unambiguously define $\mathrm{red}(a)$, the *reduction* of a, as the unique reduced word with $a \to \mathrm{red}(a)$. We then define $FG(X)$ as the set of *reduced* words in $X \cup X'$ and the group operation as $a \cdot b := \mathrm{red}(ab)$, where the multiplication on the right-hand side is performed in the monoid $FM(X \cup X')$; in other words, we concatenate. (I'll drop the dot to denote the product in $FG(X)$ very soon, but it is convenient for the purposes of the following discussion.)

To see that this operation is associative, just keep track of how $(a \cdot b) \cdot c$, say, is obtained: we concatenate ab, then reduce this word, then tack on c on the right, and then reduce the whole word until the process stops. Now this first set of reduction steps, on ab, could have been performed *after* attaching c on the right; c then simply acts as a spectator during this first stage. When we're done with this, we then perform our reduction steps on the whole word, as before. It follows that $(a \cdot b) \cdot c$ is a reduction of $(ab)c = abc$, but so is $a \cdot (b \cdot c)$, by the same argument. Now Lemma 3.9 shows that $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

It is clear that the empty word (is reduced and) still functions as the neutral element. Moreover, every $a = a_1 \dots a_n \in FG(X)$ has an inverse, which is given by $a^{-1} = a_n' \dots a_1'$ (and here we must interpret $(x')'$ as x). In particular, $a = x$ has inverse x' if $x \in X$.

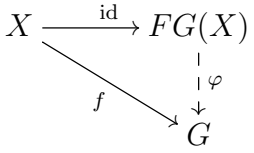
We have shown that $FG(X)$ is a group, and it is also clear that this group is generated (as a group, not as a monoid!) by X. We can now abandon the prime notation and describe $FG(X)$ as the set of all reduced words in x, x^{-1}, $x \in X$, where a single reduction step consists of striking out a two-letter subword xx^{-1} or $x^{-1}x$. The group operation is concatenation plus reduction. For example,

$$(xyxy^{-1}z)(z^{-1}yxy) = xyxxy.$$

I hope these somewhat lengthy considerations didn't make you too dizzy. Let me emphasize one more time that the whole construction is completely straightforward and obvious: if you want $x \in X$ to generate a group with no unnecessary relations, well, just multiply the generators and their inverses formally and declare all these words to be distinct (= no relations!), except of course for occurrences of xx^{-1} or $x^{-1}x$, which you must be allowed to cancel. This is really all we did; it's just the proper formal set-up that becomes mildly tedious.

As expected and intended, the analog of Theorem 3.7 holds:

Theorem 3.11. *Let X be a set and let G be a group. Then, given any map $f : X \to G$, there exists a unique homomorphism $\varphi : FG(X) \to G$ such that $f = \varphi \circ \mathrm{id}$, where $\mathrm{id}(x) = x$ (interpreted as a one letter word).*



Proof. This is the same proof as in the monoid case. Since we must define $\varphi(x) = f(x)$ for $x \in X$, just to make the diagram commutative, we obtain from Proposition 3.8 that φ is unique as a homomorphism. More explicitly, if $a = a_1 \dots a_n$ with $a_j \in X$ or $a_j^{-1} \in X$, we must set $\varphi(x) = f(a_1) \cdots f(a_n)$, where we have extended f to $X \cup X^{-1}$ in the obvious way, by setting $f(x^{-1}) = f(x)^{-1}$ for $x \in X$. Again, it is now easy to check that this φ works: write $a = a_1 \dots a_m$, $b = b_1 \dots b_n$. Then

$$\varphi(a)\varphi(b) = f(a_1) \dots f(a_m) f(b_1) \dots f(b_n), \tag{3.2}$$

and we obtain $\varphi(ab)$ by reducing ab, which amounts to deleting some of the a's and b's, and then we form a similar product of factors $f(a_j)$, $f(b_j)$. It now suffices to observe that each individual reduction step removes two factors whose counterparts on the right-hand side of (3.2) produce a 1 when multiplied together. In other words, this right-hand side is unaffected by the reduction, and thus $\varphi(ab) = \varphi(a)\varphi(b)$, as required. □

Corollary 3.12. *Let G be a group with a set of generators $X \subseteq G$. Then there is a surjective homomorphism $\varphi : FG(X) \to G$, and $G \cong FG(X)/K$ for some $K \trianglelefteq FG(X)$.*

Proof. Take $f(x) = x$ in Theorem 3.11. (Why is φ surjective?) □

In this form, it almost looks as if each group G with generating set X came with its own private free group $FG(X)$ that can be mapped onto it, but of course this is not the case because it is completely irrelevant what names exactly we give to the generators of a free group. More precisely, $FG(X) \cong FG(Y)$ if (and only if, but we won't discuss this here) there is a bijection $f : X \to Y$.

Exercise 3.11. Show this.

In particular, for each integer $n \geq 1$, there is a unique, up to isomorphism, free group $FG_n = FG(x_1, \ldots, x_n)$ with this many generators. Any group whatsoever that is generated by n of its elements is a homomorphic image of FG_n.

Exercise 3.12. Show that $FG(X)$ is again characterized by the mapping property from Theorem 3.11. More precisely, suppose that $j : X \to F$ is a map into a group F such that if $f : X \to G$ is any map into a group G, then there exists a unique homomorphism $\varphi : F \to G$ with $\varphi \circ j = f$. Prove that then $F \cong FG(X)$.

3.3. **Generators, relations, and presentations.** Let G be a group that is generated by $X \subseteq G$. Then, as we saw in Proposition 2.9, the general element $a \in G$ is a product ("word") in the generators and their inverses, say $a = a_1 a_2 \cdots a_n$, with $a_j \in X \cup X^{-1}$. In general, there is no reason to assume that two such products will represent distinct elements of G even if they are distinct as elements of $FG(X)$. Rather, there will be *relations* $a = b$ between distinct words.

Maybe we can conveniently describe groups in this way, by giving generators and relations. In principle, this is certainly possible: if all else fails, we can just take the whole group $X = G$ as the generating set and list all evaluations $ab = c$, $a, b \in G$, as relations. Of course, this is silly; we are really trying to keep both the set of generators and the set of relations small and manageable.

Let's make this more formal. Let X be a set. We now define a *relation* on X simply as a pair $(x, y) \in FG(X) \times FG(X)$; the intended interpretation is the identity $x = y$, and in fact we will usually write relations in this way. Now given a set X and relations, can we build a group that is generated by X and satisfies the relations we imposed, but no unnecessary additional relations? This is in fact quite easy to

do for us now because we have the free group $FG(X)$ as a convenient starting point; we can think of this as a group with no relations. The new group we are trying to construct will also be generated by X, so it will be $FG(X)/K$ for suitable $K \trianglelefteq FG(X)$. For each relation (x, y), we must certainly insist that $\overline{x} = \overline{y}$ in $FG(X)/K$, or, equivalently, that $xy^{-1} \in K$; otherwise we are not satisfying this relation. This suggests to define K as the smallest normal subgroup of $FG(X)$ with $xy^{-1} \in K$ for all relations (x, y).

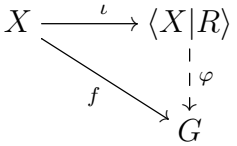
Exercise 3.13. Show that this definition makes sense. More generally, show that if A is a subset of a group G, then there exists a smallest normal subgroup K with $K \supseteq A$. (Perhaps read the first few paragraphs of Section 2.3 again if you don't have the right idea.)

Definition 3.13. Let X be a set and let R be a set of relations on X. Then we define $\langle X|R\rangle = FG(X)/K$, where K is the smallest normal subgroup of $FG(X)$ that contains xy^{-1} for all $(x, y) \in R$.

This is a group that is generated by X, or it would be more correct to say that $G = \langle X|R\rangle$ is generated by $\{xK : x \in X\}$ (X is, strictly speaking, not even a subset of G). Moreover, all relations $(x, y) \in R$ hold in G in the sense that $xK = yK$. Finally, just like the free group itself, G does not have unnecessary relations, by which we mean relations other than the ones in R and those implied by those in R (of course, what is or isn't implied by R may be far from obvious in a given concrete case).

This last property found its expression in universal mapping properties in the case of the free group, so it's reasonable to expect something similar for G.

Theorem 3.14 (Dyck)**.** *Let R be a set of relations on X, and let $f : X \to G$ be a map to a group G that preserves all relations: $f(x) = f(y)$ for all $(x, y) \in R$. Let $\iota : X \to \langle X|R\rangle$ be the inclusion map $\iota(x) = xK$. Then there exists a unique homomorphism φ such that the following diagram commutes:*



The proof is straightforward, but I want to skip it here. (Do it if you are interested: first map the free group $FG(X)$ into G, then factor through $FG(X)/K$.)

As before, the most interesting application of the theorem is the special case $X \subseteq G$, $G = \langle X\rangle$, $f(x) = x$. Then Dyck's Theorem says

that $\langle X|R\rangle$ can be mapped homomorphically onto any group that is generated by X and satisfies all relations in R.

This way of writing a group $G = \langle X|R\rangle$ in terms of generators and relations is called a *presentation* of G (don't confuse this with *re*presentations of groups, which are something else entirely). Presentations are useful tools. Also recall that every group has a presentation; in fact, it has (infinitely) many. For example, you can gratuitously add unneeded generators and then impose relations saying that these are really equal to some other generators. We are of course mainly interested in economic presentations that make do with few generators and relations.

Example 3.1. Let's start out with the case of just one generator, let's say a. So we are now dealing with cyclic groups. Reduced words in a, a^{-1} must consist of only a's or only a^{-1}'s (why?), and from this you can deduce quickly that $FG(a) \cong \mathbb{Z}$, and the isomorphism can send a to $1 \in \mathbb{Z}$ (do it please). So $\mathbb{Z}$ itself has the presentation $\mathbb{Z} \cong \langle a|\ \rangle$ (one generator, no relations). As for the other cyclic groups, recall that $\mathbb{Z}_k \cong \mathbb{Z}/k\mathbb{Z}$ and $k\mathbb{Z}$ is generated by k, so $\mathbb{Z}_k \cong \langle a|a^k = 1\rangle$, as could have been guessed right away.

Example 3.2. Let's now take n generators $a_1, \dots, a_n$, and let's make the group abelian by imposing the relations $a_j a_k = a_k a_j$, $j \neq k$. What is this group $G = \langle a_1, \dots, a_n | a_j a_k = a_k a_j\rangle$? Thanks to these relations, I can freely rearrange the a_j in any word, so an arbitrary element of G can be represented by a word of the form $a_1^{N_1} \dots a_n^{N_n}$, with $N_j \in \mathbb{Z}$. This gives an isomorphism $G \cong \mathbb{Z}^n$; the group operation on $\mathbb{Z}^n$ is of course componentwise addition.

Exercise 3.14. Provide more details please. In particular, explain why this group is really abelian; why can I also move inverses of generators anywhere in a word?

When dealing with presentations, it is convenient to not overload the notation by writing elements of $G = \langle X|R\rangle$ also as words in the generators and their inverses (strictly speaking, they are elements of a quotient $FG(X)/K$), and we have done this here already. You could also think of the presented group in terms of words that are subjected to a rewriting mechanism, somewhat reminiscent of how we obtained the free group as words plus a reduction process. In fact, the analogy is complete: you can view the free group $FG(X)$ as the free monoid $FM(X \cup X')$ with the relations $xx' = x'x = 1$. However, recognizing whether or not two words represent the same element of a group $\langle X|R\rangle$

can be arbitrarily difficult, whereas the reduction in the construction of $FG(X)$ is straightforward and algorithmic.

Example 3.3. Now let's try to find a presentation of the symmetric group S_3. We know from Exercise 2.63(b) that S_3 is generated by $a = (123)$ and $b = (12)$. Clearly these satisfy $a^3 = b^2 = 1$. Also, $ab = (13)$, so $(ab)^2 = 1$, and this can be rewritten as $a^2b = ba$. I now claim that these three relations suffice: $S_3 \cong \langle a, b | a^3 = b^2 = 1, a^2b = ba \rangle$.

Let G be this group. I claim that every element of G can be written as $a^n b$ or a^n, with $n = 0, 1, 2$. To see this, first notice that we don't need inverses of generators in our words because $a^{-1} = a^2$, $b^{-1} = b$. I can then use the last relation to move all b's in a word to the right: start with the rightmost b (also, since $b^2 = 1$, we never need two or more consecutive b's), move this past its right neighbor a, and repeat this step to eventually arrive at $a^n b$ or a^n, as claimed.

This list has only 6 entries, so $|G| \leq 6$. We might now actually get worried that G might be even smaller due to other consequences of our relations that we haven't discovered yet, but that is not the case because S_3 is a group that satisfies our relations. In fact, that is how we got them in the first place. Now $|S_3| = 6$, and this means that G cannot be smaller than this or we would run into a contradiction to the mapping property from Dyck's Theorem. In fact, we also obtain a homomorphism $\varphi : G \to S_3$ by mapping, as expected, $a \mapsto (123)$, $b \mapsto (12)$. This is surjective because the image contains the generators of S_3, and it is injective because G only has 6 elements which must be mapped to the 6 elements of S_3. So $G \cong S_3$, as claimed.

Alternatively, you could just reconstruct the multiplication table, as follows: $a^m a^n = a^{m+n}$, and here you are expected to reduce $m + n$ modulo 3. Similarly, $a^m(a^n b) = a^{m+n}b$. Next, $(a^m b)a^n = a^N b$, where you find N from the process of moving b through to the right that was described above. Similarly, $(a^m b)(a^n b) = a^N$, with an N that you can in principle find from m, n. You now have the 6 words $1, a, a^2, b, ab, a^2b$ and a binary operation on this set, and it is now easy in principle, if incredibly tedious, to check that this is a group that will then also turn out to be isomorphic to S_3.

This last example cautions us that the structure of a group may not be obvious at all from its presentation because the relations could have consequences that are not immediately obvious. As a trivial illustration, consider the group $G = \langle a | a^{10} = 1, a^{63} = 1 \rangle$. We know that $a^n = 1$ precisely if n is a multiple of $o(a)$. Since 10 and 63 are relatively prime, it follows that $o(a) = 1$, so $G = \{1\}$. This was easy to see through, but of course these things can get arbitrarily complicated, and in fact it

has been shown that many groups have an algorithmically *unsolvable word problem:* this means, roughly speaking, that you cannot write a computer program that accepts two words in the generators as input and outputs the correct yes/no-answer to the question *do the two words represent the same group element?* after a terminating computation.

Exercise 3.15. Use arguments similar to the ones from Example 3.3 to determine the structure of the group $G = \langle a, b | a^3 = b^2 = 1, ab = ba \rangle$.

Exercise 3.16. Analyze $G = \langle a, b | ab = b^2 a, ba = a^2 b \rangle$.

The *dihedral group* D_n is defined as the group of symmetries of the regular n-gon. More formally, we can view D_n as the finite subgroup of $GL(2, \mathbb{R})$ with the elements

$$R_j = \begin{pmatrix} \cos 2\pi j/n & -\sin 2\pi j/n \\ \sin 2\pi j/n & \cos 2\pi j/n \end{pmatrix}, \qquad j = 0, 1, \ldots, n-1$$

("rotations") and

$$S_j = \begin{pmatrix} \cos 2\pi j/n & \sin 2\pi j/n \\ \sin 2\pi j/n & -\cos 2\pi j/n \end{pmatrix}, \qquad j = 0, 1, \ldots, n-1$$

("reflections").

Exercise 3.17. (a) Confirm that D_n is indeed a group.
(b) Show that $D_n \cong \langle a, b | a^n = b^2 = 1, ab = ba^{-1} \rangle$.

3.4. **Group actions.** Recall that given a set X, we defined $S(X)$ as the group of all bijections on X. An *action* of a group G on a set X can be defined as a homomorphism $\varphi : G \to S(X)$. It is also possible (and more common) to give a slightly more explicit definition by taking this apart, as follows: Notice, first of all, that from an action of G on X, we obtain a map from $A : G \times X \to X$, by setting $A(g, x) = \varphi(g)(x)$. Then, since φ is a homomorphism, we obtain that $A(1, x) = x$ and $A(gh, x) = A(g, A(h, x))$.

Conversely, if a map $A : G \times X \to X$ has these two properties, then we obtain a homomorphism $\varphi : G \to S(X)$ by defining $\varphi(g)(x) = A(g, x)$.

Exercise 3.18. Prove this.

These remarks lead to the following reformulation of our original definition. We now drop A in the notation.

Definition 3.15. We say that a group G *acts* on a set X if there is a map $G \times X \to X$, $(g, x) \mapsto gx$ such that

$$1x = x, \quad (gh)x = g(hx) \qquad (g, h \in G, x \in X).$$

Exercise 3.19. Prove directly from this definition that $x \mapsto gx$ is a bijection on X for arbitrary fixed $g \in G$.

Group actions are ubiquitous and often arise very naturally. For example, matrices really "want" to act on vectors, so it's natural to try to let $G = GL(2, \mathbb{R})$, say, act on $X = \mathbb{R}^2$ by simply multiplying $g \in G$ and $x \in X$ as matrices. This is a group action: the neutral element of G is the identity matrix $1 = \mathrm{diag}(1, 1)$, which does have the property that $1x = x$ for $x \in \mathbb{R}^2$, and $(gh)x = g(hx)$ follows from the associativity of the matrix product.

Similarly, the dihedral group D_n acts on the n vertices $X = \{1, \ldots, n\}$ (for convenience labeled by integers here) of a regular n-gon in a natural way, and the symmetric group S_n acts on $\{1, 2, \ldots, n\}$.

Example 3.4. A group G acts on itself in various ways: by left multiplication $(g, x) \mapsto gx$, $g, x \in G$ or by right multiplication $(g, x) \mapsto xg^{-1}$, or by *conjugation* $(g, x) \mapsto gxg^{-1}$. We used the action by left multiplication in our proof of Cayley's Theorem.

Exercise 3.20. Show that these are indeed group actions.

The set $Gx = \{gx : g \in G\}$ is called the *orbit* of $x \in X$. A group action is called *transitive* if $Gx = X$ for all orbits.

Exercise 3.21. Show that this will hold as soon as $Gx = X$ for *some* orbit.

Exercise 3.22. Show that $GL(2, \mathbb{R})$ acts transitively on $\mathbb{R}^2 \setminus \{0\}$, and the action of a group G on itself by left or right multiplication is transitive, while the action of G on itself by conjugation is never transitive, unless $G = \{1\}$.

The *stabilizer* of a point $x \in X$ is defined as

$$\mathrm{Stab}(x) = \{g \in G : gx = x\}.$$

Theorem 3.16. $\mathrm{Stab}(x)$ *is a subgroup of* G*, and*

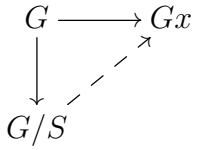
$$|Gx| = [G : \mathrm{Stab}(x)].$$

The second statement will be most interesting for finite orbits and finite index stabilizers, but it holds in general.

Proof. Notice, first of all, that if $gx = y$, then $g^{-1}y = x$ (just let g^{-1} act on both sides). So, if $g, h \in \mathrm{Stab}(x)$, then also $h^{-1} \in \mathrm{Stab}(x)$ and $(gh^{-1})x = g(h^{-1}x) = gx = x$, so $gh^{-1} \in \mathrm{Stab}(x)$ as well. This shows that $\mathrm{Stab}(x)$ is a subgroup.

To prove the second claim, fix $x \in X$, and consider the map $g \mapsto gx$. Let's also abbreviate $S = \mathrm{Stab}(x)$. Notice that $gx = hx$ precisely if

$h^{-1}g \in S$, and this happens precisely if g, h are in the same (left) coset of S. Thus we obtain an induced *injective* map $gS \mapsto gx$ from the coset space G/S to Gx.



Note that we are *not* claiming that S is a *normal* subgroup of G, and indeed this is false in general. However, we can consider the coset space $G/S = \{aS : a \in G\}$ also for an arbitrary subgroup, and this still comes with a natural surjection $G \to G/S$, $g \mapsto gS$, though we don't have a group structure on G/S if S isn't normal.

Since the original map $g \mapsto gx$ was surjective onto the orbit, it follows that the induced map is a bijection between G/S and Gx. □

Exercise 3.23. (a) Provide an example of a non-normal stabilizer.
(b) Show that $g\,\mathrm{Stab}(x)g^{-1} = \mathrm{Stab}(gx)$.

Next, we observe that a group action partitions the set acted on into orbits. Put differently, two orbits Gx, Gy are either equal or disjoint. (Obviously, since $x \in Gx$, every point of X is in some orbit.) Indeed, if $z \in Gx \cap Gy$, say $z = gx = hy$, then $x = g^{-1}hy \in Gy$, so $Gx \subseteq Gy$ and similarly $Gy \subseteq Gx$, so $Gx = Gy$. When combined with Theorem 3.16, this gives the following useful counting formula. We now focus on actions on finite sets.

Theorem 3.17. *Let the group G act on a finite set X, and pick one point x_j from each orbit. Then*

$$|X| = \sum [G : \mathrm{Stab}(x_j)]. \tag{3.3}$$

Proof. As we just observed, we have the partition $X = Gx_1 \cup \ldots \cup Gx_n$. Now use Theorem 3.16. □

These ideas are reminiscent of our proof of Lagrange's Theorem, and indeed we could view this as a special case of Theorem 3.17. To do this, let H be a subgroup of a finite group G, and let H act on $X = G$ by left multiplication. The orbit of an $x \in G$ is the corresponding right coset Hx, so the number of orbits equals the index $[G : H]$. Furthermore, $\mathrm{Stab}(x) = \{1\}$, so $[H : \mathrm{Stab}(x)] = |H|$, and now Theorem 3.17 gives that $|G| = [G : H]|H|$.

A particularly interesting application of Theorem 3.17 is obtained by considering the conjugation action of a finite group G on itself. So we send $(g, x) \mapsto gxg^{-1}$. In this case, the orbit $\{gxg^{-1} : g \in G\}$ of an

$x \in G$ is also called the *conjugacy class* of x. What is the stabilizer of an $x \in G$? We have that $gxg^{-1} = x$ precisely if $gx = xg$, that is, precisely if g and x commute. This motivates:

Definition 3.18. The *centralizer* of $x \in G$ is defined as the collection of those $g \in G$ that commute with x:

$$C(x) = \{g \in G : gx = xg\}$$

Similarly, the *center* $C = C(G)$ of a group G is defined as

$$C = \{g \in G : gx = xg \text{ for all } x \in G\} = \bigcap_{x \in G} C(x).$$

We know that $C(x)$, being a stabilizer of the conjugation action of G on itself, is a subgroup. This makes $C = \bigcap C(x)$ a subgroup as well; of course, it's also easy to check this directly. More can be said:

Exercise 3.24. Show that $C \trianglelefteq G$. Is $C(x)$ also normal?

With these preparations out of the way, we can now rephrase Theorem 3.17 for the special case of the conjugation action as follows:

Theorem 3.19 (The class equation)**.** *Let G be a finite group with center C. Pick one representative x_j from each conjugacy class with more than one element. Then*

$$|G| = |C| + \sum [G : C(x_j)].$$

Proof. Notice that the conjugacy class of an $x \in G$ consists of x only precisely if $x \in C$. Each such conjugacy class contributes a 1 to the sum from (3.3), and there are $|C|$ of these. Since $\mathrm{Stab}(x) = C(x)$ for the conjugation action, it is now clear that our identity is (3.3), slightly rewritten. □

Corollary 3.20. *Let p be a prime, and suppose that $|G| = p^n$, $n \geq 1$. Then G has a non-trivial center $C \neq \{1\}$.*

Exercise 3.25. Show that $G = S_n$, $n \geq 3$, has center $C = \{1\}$.

Proof. Consider the class equation for G. For each $C(x)$ occuring in the sum (which, incidentally, could be empty, but then $G = C$ and we're done), we have that $C(x) \neq G$ (why?). This implies that p divides $[G : C(x)]$. Since also $p||G|$, it follows that $|C|$ must also be divisible by p, and thus $|C| \geq p$, as claimed. □

Exercise 3.26. (a) Let G be a group with center C. Show that if G/C is cyclic, then G is an abelian group.
(b) Let p be a prime, and suppose that $|G| = p^2$. Show that G is abelian. *Suggestion:* Consider the center C of G and G/C.

Exercise 3.27. Give an example of a non-abelian group G that has a normal subgroup K, such that both K and G/K are abelian.

Exercise 3.28. Show that there are non-abelian groups of order p^3, p a prime. *Suggestion:* Try to find a non-abelian group of order 8 among our examples.

Exercise 3.29. Suppose that $|G| = p^n$, p a prime, and $H \trianglelefteq G$, $H \neq \{1\}$. Show that then $H \cap C \neq \{1\}$. *Suggestion:* Try to adapt the proof of Corollary 3.20 (the Corollary is the special case $H = G$ of this exercise).

Exercise 3.30. Let H be a subgroup of G with $[G : H] = n$. Show that there is a *normal* subgroup $K \trianglelefteq G$, $K \subseteq H$, such that $[G : K] | n!$. *Suggestion:* Let G act on the (left) coset space G/H by left multiplication $(g, aH) \mapsto gaH$, and consider the kernel of the associated homomorphism $\varphi : G \to S(G/H)$.

Exercise 3.31. Let p be the smallest prime divisor of $|G|$. Show that a subgroup of index p is normal. *Suggestion:* Apply the result from the previous Exercise.

Exercise 3.32. Decompose a permutation $\pi \in S_n$ into disjoint cycles, such that every integer $1 \leq j \leq n$ is in exactly one cycle. Denote the lengths of these cycles by $\ell_1 \geq \ell_2 \geq \ldots \geq \ell_k$, in decreasing order. Now prove that two permutations π, π' are in the same conjugacy class precisely if they have the same cycle structure in the sense that $k = k'$, $\ell_j = \ell'_j$, $j = 1, 2, \ldots, k$.

Given a general group G, one might hope to analyze its structure by breaking it into smaller pieces and studying those pieces separately. More specifically, this could be done by finding a normal subgroup K, and this gives us the smaller groups K and G/K. The basic building blocks in this process would then be groups with no normal subgroups at all, other than $K = \{1\}$ and $K = G$. Such groups are called *simple* groups.

The classification of the finite simple groups has indeed been completed. It was one of the largest (it's probably safe to say: *the* largest) projects of 20th century mathematics. That still leaves us with the second step of reassembling G from its pieces. More specifically, if K and G/K are known, up to isomorphism, can we reconstruct G, also up to isomorphism, from this information? For other algebraic structures (for example, vector spaces), this works, but in the case of groups, the answer is a very loud *no.*

This is in fact clear from very basic examples. The *direct product* of two groups G, H is defined in the expected way as $G \times H$, endowed

with the group operation $(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$. Now consider $G_1 = \mathbb{Z}_2 \times \mathbb{Z}_2$ and $G_2 = \mathbb{Z}_4$.

Exercise 3.33. Show that both groups G_j have normal subgroups $K_j \trianglelefteq G_j$ such that $K_j \cong \mathbb{Z}_2$, $G_j/K_j \cong \mathbb{Z}_2$. However, $G_1 \ncong G_2$.

The notion of a *semidirect product* of groups will shed some more light on this issue, and it is of independent interest. An *automorphism* of a group G is a bijective homomorphism of G onto itself. Equivalently, an automorphism is a map $\varphi \in S(G)$ that is a homomorphism. I mention in passing that the automorphisms of G form a subgroup $\mathrm{Aut}(G)$ of $S(G)$. We say that a group H *acts* on the group G *by automorphisms* if H acts on G and, moreover, for each $h \in H$, the map $g \mapsto hg$ is an automorphism of G (it is automatically a bijection, coming from a group action, so the extra requirement is that $g \mapsto hg$ is a homomorphism of G).

Definition 3.21. Let H act on G by automorphisms. Then the *semidirect product* $G \rtimes H$ of G and H is defined as the set $G \times H$, endowed with the group operation

$$(g_1, h_1)(g_2, h_2) = (g_1(h_1 g_2), h_1 h_2).$$

Here, we are of course *not* multiplying $h_1 g_2$, which wouldn't make sense since $h_1 \in H$, $g_2 \in G$ come from different groups; rather, h_1 acts on g_2 to produce another element of G, which is then multiplied by $g_1 \in G$.

Notice that the semidirect product depends on three data: the two groups G and H, plus the action of H on G.

Exercise 3.34. Verify that this operation is associative, $(1, 1)$ is a neutral element, and each $(g, h) \in G \rtimes H$ has an inverse, which is given by $(h^{-1}g^{-1}, h^{-1})$. (In other words, $G \rtimes H$ is indeed a group.) Also, show that if H acts trivially, that is, $hg = g$, then $G \rtimes H \cong G \times H$.

So direct products are special semidirect products, with the trivial action $hg = g$, but there are other examples.

Example 3.5. Let $\mathbb{Z}_2$ act on $\mathbb{Z}_n$ by mapping $(1, k) \mapsto -k$, $k \in \mathbb{Z}_n$ (and of couse $(0, k) \mapsto k$). Since $-(k+j) = (-j)+(-k)$ in $\mathbb{Z}_n$ (or any group, for that matter), this is an action by automorphisms. So we can form the semidirect product $G = \mathbb{Z}_n \rtimes \mathbb{Z}_2$ based on this action. I claim that $G \cong D_n$, the dihedral group. We saw earlier that

$$D_n \cong \langle a, b | a^n = b^2 = 1, bab = a^{-1} \rangle.$$

Both D_n and G have $2n$ elements, so to show that $G \cong D_n$ it suffices to find two generators of G that satisfy the same relations.

Exercise 3.35. Think about this more carefully please. Why is this indeed enough? (Refer to Dyck's Theorem perhaps for a formal argument.)

It's natural to try $a = (1, 0)$, $b = (0, 1)$. These two elements do generate the semidirect product. The first two relations are obvious, and $ba = (0 + 1 \cdot 1, 1 + 0) = (-1, 1)$, so $(ba)b = (-1 + 1 \cdot 0, 1 + 1) = (-1, 0) = -a$, as required; here, the dot product $h \cdot g$ denotes the action of $\mathbb{Z}_2$ on $\mathbb{Z}_n$.

In particular, with this action, $\mathbb{Z}_n \rtimes \mathbb{Z}_2 \ncong \mathbb{Z}_n \times \mathbb{Z}_2$ (this latter group is abelian), so semidirect products are more general than direct products, and the resulting group will, in general, depend on the action.

Theorem 3.22. *Let $G \rtimes H$ be a semidirect product (the indefinite article is appropriate because of the dependence on the action). Then $G_0 = \{(g, 1) : g \in G\}$ is a normal subgroup of $G \rtimes H$. We have that $G_0 \cong G$ and $(G \rtimes H)/G_0 \cong H$.*

We conclude that if for a group G, a normal subgroup K and G/K are known, up to isomorphism, then G could still be any semidirect product of K and G/K. In fact, the notion of a semidirect product is not wide enough for this reconstruction; in general, one needs so-called *group extensions.*

Exercise 3.36. Show that any semidirect product $\mathbb{Z}_2 \rtimes \mathbb{Z}_2$ is isomorphic to the direct product. (So $\mathbb{Z}_4 \ncong \mathbb{Z}_2 \rtimes \mathbb{Z}_2$, even though $\mathbb{Z}_4$ has a normal subgroup $K \cong \mathbb{Z}_2$, $G/K \cong \mathbb{Z}_2$.)

Proof. It is obvious that G_0 is a subgroup. To see that G_0 is normal, recall that $(a, h)^{-1} = (\dots, h^{-1})$. It is now also immediate that $(a, h)(g, 1)(a, h)^{-1} \in G_0$, simply because in the second component, we are multiplying $h1h^{-1} = 1$, as required.

Clearly, $G_0 \cong G$, via the obvious isomorphism $(g, 1) \mapsto g$. Finally, $(g, h)G_0 = (g', h')G_0$ precisely if $(g, h)(g', h')^{-1} \in G_0$, and this happens precisely if $h = h'$. This observation gives an isomorphism $H \to (G \rtimes H)/G_0$, by mapping $h \mapsto (1, h)G_0$. □

Exercise 3.37. Show that $G \rtimes H$ always has a subgroup isomorphic to H. However, show that there need not be a *normal* subgroup $\cong H$. *Suggestion:* Work with the dihedral group for a counterexample.

3.5. **The Sylow Theorems.** Throughout this section, all groups will be assumed finite. We know from Lagrange's Theorem that the order of a subgroup H of G divides $|G|$. Conversely, if n divides $|G|$, will there be a subgroup H of G of order n? It turns out that this is not always the case.

Theorem 3.23. *A_4 has no subgroup of order 6.*

Recall that A_n denotes the alternating group, that is, the subgroup of S_n consisting of the even permutations. Since $[S_n : A_n] = 2$, we have that $|A_n| = |S_n|/2 = n!/2$, so in particular $|A_4| = 12$.

Proof. If there were a subgroup H of order 6, then $[A_4 : H] = |A_4|/6 = 2$, so H would be normal in A_4, and the quotient group A_4/H has order 2. So for any $\pi \in A_4$, it would follow that $(\pi H)^2 = \overline{1}$ or, equivalently, $\pi^2 \in H$. This implies that for any 3 cycle $\pi = (jkm)$, we have that $\pi = \pi^4 = (\pi^2)^2 \in H$. However, there are 8 distinct 3 cycles $(123), (213), (124), \ldots$, so $|H| \geq 8$, and we have reached a contradiction. □

However, if a divisor of $|G|$ has only one prime factor, then there will always be a subgroup of this order.

Theorem 3.24 (Sylow I)**.** *Let p be a prime, and suppose that $p^k||G|$. Then G has a subgroup of order p^k.*

The proof will be based on the following

Lemma 3.25. *Let G be an abelian group with $p||G|$, p a prime. Then G has an element of order p.*

Proof. We will do this by induction on $|G|$. Of course, this is trivially true for $|G| = 1$ (and $= 2, 3$). Now assume the claim for all groups of order $< |G|$, and suppose that $p||G|$. Take an arbitrary $a \in G$, $a \neq 1$. If $p|o(a)$, let's say $o(a) = pn$, then a^n will work. Otherwise, $(p, o(a)) = 1$, and this means that $|G/\langle a\rangle| = |G|/o(a)$ is still divisible by p. Moreover, since $a \neq 1$, this group has smaller order than G, so by the induction hypothesis, we can find an element $b\langle a\rangle$, $b \in G$, of order p. Let's write $n = o(b)$ for the order of b in G. Then $(b\langle a\rangle)^n = b^n\langle a\rangle = \langle a\rangle = \overline{1} \in G/\langle a\rangle$, so $p|o(b)$, and we're back in the case we already discussed. □

Proof of Theorem 3.24. We again proceed by induction on $|G|$. So assume the claim for all groups of order $< |G|$. Consider the class equation

$$|G| = |C| + \sum [G : C(x_j)].$$

If $p \nmid |C|$, then also $p \nmid [G : C(x_j)]$ for at least one of the summands, but this means that $p^k||C(x_j)|$. Now the induction hypothesis lets us find a subgroup $H \subseteq C(x_j)$ of order p^k, and we are done in this case. (Why is $C(x_j)$ a group of smaller order than G?)

If $p||C|$, then we apply the lemma to C to find a $c \in C$, $o(c) = p$. Since $\langle c\rangle \subseteq C$, the subgroup $\langle c\rangle$ is normal, and we can form the quotient $G/\langle c\rangle$. This is a group of order $|G|/p$, so the induction hypothesis

produces a subgroup $\overline{H} \subseteq G/\langle c\rangle$ of order p^{k-1}. By the first isomorphism theorem, this subgroup is of the form $\overline{H} = H/\langle c\rangle$, for some subgroup $\langle c\rangle \subseteq H \subseteq G$. Now observe that

$$|H| = [H : \langle c\rangle]|\langle c\rangle| = |\overline{H}|p = p^{k-1}p = p^k,$$

so H is a subgroup of the type we are looking for. □

A subgroup of this type, with k maximal, is called a *Sylow p-subgroup.* We denote the collection of Sylow p-subgroups by $\mathrm{Syl}_p(G)$; we may drop G here if the underlying group is clear from context or irrelevant. So if $|G| = p^n m$ with $(p, m) = 1$, then $H \in \mathrm{Syl}_p(G)$ precisely if H is a subgroup of order p^n. Sylow's first theorem says that there always is such a subgroup.

Theorem 3.26 (Sylow II)**.** *(a) Any two Sylow p-subgroups are conjugate: if $P_1, P_2 \in \mathrm{Syl}_p(G)$, then $P_2 = aP_1a^{-1}$ for some $a \in G$.*

(b) Write $N = |\mathrm{Syl}_p(G)|$ and $|G| = p^n m$, $(p, m) = 1$. Then $N|m$ and $N \equiv 1 \mod p$.

(c) Any subgroup of order p^k is contained in a Sylow p-subgroup.

The key idea will be to let G act on Syl_p by conjugation: $(g, P) \mapsto gPg^{-1}$.

Exercise 3.38. Check that indeed $gPg^{-1} \in \mathrm{Syl}_p$ again and that this defines an action.

The stabilizer of a $P \in \mathrm{Syl}_p$ is given by $\{g \in G : gPg^{-1} = P\}$. This is called the *normalizer* of P and denoted by $N(P)$. Observe that $N(P)$ is a subgroup (being a stabilizer), and that $P \trianglelefteq N(P)$.

Lemma 3.27. *Let $P \in \mathrm{Syl}_p(G)$, and suppose that $H \subseteq N(P)$ is a subgroup of order p^k, $k \geq 0$. Then $H \subseteq P$.*

Proof. As we just observed, $P \trianglelefteq N(P)$. Now the second isomorphism theorem gives that $HP/P \cong H/(H \cap P)$. This in particular shows that HP/P has order p^j, so $|HP| = p^j|P|$. Since the order of P is the highest possible power of p of a subgroup of G, it follows that $j = 0$, so $HP = P$ and thus $H \subseteq P$, as claimed. □

We are now ready for the

Proof of Theorem 3.26. As planned, we let G act on Syl_p by conjugation. Let $S \subseteq \mathrm{Syl}_p$ be one of the orbits of this action. For any subgroup $P \subseteq G$ we then also obtain an action of P on S, simply by restricting. If we take a $P \in S$, then $\{P\}$ is an orbit of this restricted action. Moreover, this is the only orbit consisting of a single point: if $\{P'\}$, $P' \in S$,

is an orbit under the P action, then $P \subseteq N(P')$, and now Lemma 3.27 implies that $P = P'$.

By Theorem 3.16, the cardinality of any such orbit, not consisting of a single point, is divisible by p. Thus the counting technique from Theorem 3.17 shows that $|S| \equiv 1 \mod p$.

On the other hand, if we pick a Sylow p-subgroup $P \notin S$, then the same argument shows that $|S| \equiv 0 \mod p$. This contradiction can only be avoided if there are no such $P \notin S$. We have shown that $S = \mathrm{Syl}_p$. In other words, the action of G on Syl_p by conjugation is transitive, and this is what part (a) claims. We also just proved that $N \equiv 1 \mod p$. Moreover, by Theorem 3.17 again, $N = [G : N(P)]$, and since $N(P) \supseteq P$, this is a divisor of m, as claimed.

It remains to establish part (c). So let H be a subgroup of G of order p^k. Let H act on Syl_p by conjugation. The cardinality of an orbit is $[H : T]$, where $T \subseteq H$ is a stabilizer. So the cardinality of an arbitrary orbit is a power of p. Since $N \equiv 1 \mod p$, there must be at least one orbit of cardinality 1. In other words, $H \subseteq N(P)$ for some $P \in \mathrm{Syl}_p$. Now Lemma 3.27 shows that $H \subseteq P$. □

Exercise 3.39. Suppose that a group G has exactly one element x of order 2. Show that $x \in C(G)$.

The Sylow theorems sometimes impose strong restrictions on the structure of finite groups. Here are some typical applications:

Example 3.6. There is no simple group of order pq, p, q both primes. To show this, consider Syl_p and $N = |\mathrm{Syl}_p|$; for convenience, let's assume that p is the larger of the two primes. (In fact, since any $P \in \mathrm{Syl}_p$ has index $[G : P] = q$, which is the smallest prime divisor of $|G|$, the claim already follows from Exercise 3.31; here we give an independent argument.) Theorem 3.26(b) says that $N|q$ and $N \equiv 1 \mod p$. Since q is a prime, the first condition really says that $N = 1$ or $N = q$, but only $N = 1$ is consistent with the second condition. This unique $P \in \mathrm{Syl}_p$ must be invariant under conjugation and thus normal.

Exercise 3.40. This discussion implicitly assumed that $p \neq q$. Show that no group of order p^n, p a prime, $n \geq 2$, is simple.

Example 3.7. For a somewhat more elaborate example of the same technique, I now want to show that there is no simple group of order 80. Notice that $80 = 2^4 \cdot 5$, and consider again Syl_5 and $N = |\mathrm{Syl}_5|$. As in the previous example, we have that $N|16$, $N \equiv 1 \mod 5$. The values of N consistent with these conditions are $N = 1$, $N = 16$. In the first case, we are done because then the unique Sylow 5-subgroup

is normal. In the second case, notice that $P \cap P' = \{1\}$ for any two distinct Sylow 5-subgroups. This follows because a group of order 5 is cyclic, and it is generated by any non-identity element, so if two such subgroups have a non-identity element in common, then they are the same subgroup. It now follows that $\bigcup P$, with the union taken over $P \in \mathrm{Syl}_5$, has 65 elements: the $P \setminus \{1\}$ are pairwise disjoint and thus contribute $16 \cdot 4 = 64$ elements, and then there's 1 for one additional element. Now a Sylow 2-subgroup Q can not contain any non-identity element from $\bigcup P$ because these all have order 5 which does not divide $|Q| = 16$. So the elements of Q are exactly those 15 not in $\bigcup P$, plus the identity. In particular, there is only one Sylow 2-subgroup, which then must be normal.

Another satisfying application of the tools we have developed is the classification of finite groups of small order. Let me give two sample results here. First of all, recall that a group of order p, p a prime, is cyclic. So we know the groups of order $2, 3, 5, 7, 11, \ldots$. Let's now fill a few of the gaps.

Exercise 3.41. Suppose that $|G| = 4$. Show that $G \cong \mathbb{Z}_4$ or $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Next would be groups of order 6. We can show a more general result right away.

Theorem 3.28. *Suppose that $|G| = 2p$, p a prime. Then $G \cong \mathbb{Z}_{2p}$ or $G \cong D_p$.*

Recall that the dihedral group has the presentation

$$D_p = \langle a, b | a^p = b^2 = 1, bab = a^{-1} \rangle.$$

Proof. The case $p = 2$ was just dealt with in an exercise (provided that you also show that $D_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$; please do it). So we can assume that $p \geq 3$. Pick a Sylow p-subgroup A and a Sylow 2-subgroup B. Since these have prime orders, they are cyclic, and we can pick generators $a \in A$, $b \in B$. So $o(a) = p$, $o(b) = 2$. Since $[G : A] = 2$ and $b \notin A$, we have that $G = A \cup bA$, so a, b together generate G. It also follows that A is normal. This implies that $bab = bab^{-1} = a^k$ for some $0 \leq k < p$. We deduce from this that

$$a = bbabb = ba^k b = (bab)^k = a^{k^2},$$

or, equivalently, $a^{k^2-1} = 1$. So $o(a) = p$ must divide $k^2 - 1 = (k - 1)(k + 1)$, and since p is prime, it divides either $k - 1$ or $k + 1$. If $p | k - 1$, then $a^k = a$, so $bab = a$ or $ab = ba$. To summarize: in this first case, our group G of order $2p$ is generated by a, b, and these generators

satisfy the relations $a^p = b^2 = 1$, $ab = ba$. It's now easy to see that: (1) $\langle a, b | a^p = b^2 = 1, ab = ba\rangle \cong \mathbb{Z}_{2p}$; (2) G is isomorphic to this group.

Exercise 3.42. Provide the details please.

In the other case, $p|k+1$, it follows that $a^k = a^{-1}$, so $bab = a^{-1}$, and in addition to this, we have the two relations $a^p = b^2 = 1$. In other words, we have exactly the defining relations of the dihedral group, and our group G not only satisfies the relations of D_p but it also has the same number of elements of D_p. This implies that $G \cong D_p$ in this case (again, provide the details perhaps). □

Exercise 3.43. Well, isn't $\mathbb{Z}_p \rtimes \mathbb{Z}_2$ a group of order $2p$ for an arbitrary action of $\mathbb{Z}_2$ on $\mathbb{Z}_p$ by automorphisms? Or how about $\mathbb{Z}_2 \rtimes \mathbb{Z}_p$? Explain why this is compatible with Theorem 3.28.

Exercise 3.44. Explain how Theorem 3.28 implies that $S_3 \cong D_3$, and then prove this result directly.

Exercise 3.45. Suppose that every element $a \in G$, $a \neq 1$, has order 2. Show that G is abelian.

Exercise 3.46. Show that if G is an *abelian* group of order 8, then $G \cong \mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, or $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

We now take a look at groups of order 8. The abelian groups of this order have just been dealt with in Exercise 3.46. In the non-abelian case, a new group makes an appearance here; it has the presentation

$$Q = \langle a, b | a^4 = 1, b^2 = a^2, bab^{-1} = a^{-1}\rangle.$$

This is called the *quaternion group* because Q can be realized as a certain subgroup of the multiplicative group of the quaternions (which we'll discuss briefly in the next chapter). In more down-to-earth fashion, we can also realize Q as the subgroup $\langle A, B\rangle$ of $GL(2, \mathbb{C})$ that is generated by the matrices

$$A = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Exercise 3.47. Show that $|Q| = 8$, $Q \cong \langle A, B\rangle$ and that $Q \ncong D_4$. *Suggestion:* Proceed as in our analysis of the presentation of S_3 or D_n.

Theorem 3.29. *Let G be a non-abelian group of order 8. Then $G \cong D_4$ or $G \cong Q$.*

Proof. If G had only elements of order 1 or 2, then G would be abelian by Exercise 3.45. So we can find an $a \in G$ with $o(a) = 4$. Then $A = \langle a\rangle$ is an index 2 subgroup and thus normal. Pick any $b \notin A$.

Then $G = \langle a, b\rangle$. Since $|G/A| = 2$, we have that $(bA)^2 = b^2A = \overline{1}$. In other words, $b^2 \in A$, that is, $b^2 = a^k$. Here, $k = 1, 3$ are not possible because that would imply that $o(b) = 8$, making G cyclic. So $b^2 = 1$ or $b^2 = a^2$. Moreover, $bab^{-1} \in A$ since A is normal, and this element has order 4, so must equal a or a^3. The relation $bab^{-1} = a$ would make G abelian, so this is impossible.

Let's summarize: $G = \langle a, b\rangle$, $a^4 = 1$, $bab^{-1} = a^{-1}$, and either $b^2 = 1$ or $b^2 = a^2$. These are the relations of D_4 (first case) or Q (in the second case), so one of these groups can be mapped homomorphically onto G. Since all groups that are involved here have order 8, this map is an isomorphism, and thus $G \cong D_4$ or $G \cong Q$. □

Exercise 3.48. Give an example of a group G with a normal subgroup $K \trianglelefteq G$ such that G does not have a subgroup isomorphic to G/K. *Suggestion:* Try $G = Q$. You can then either try to find a suitable $K \trianglelefteq Q$, or you can try to find a surjective homomorphism $\varphi : Q \to H$, with H not isomorphic to a subgroup of Q.

3.6. **Normal series and composition series.**

Definition 3.30. A *normal series* for a group G is a finite sequence of descending subgroups, such that

$$G = G_1 \rhd G_2 \rhd G_3 \rhd \ldots \rhd G_n = 1.$$

The notation $G \rhd K$ means that $G \trianglerighteq K$, $G \neq K$. I also wrote 1 instead of the more accurate, but less pleasing to the eye $\{1\}$ for the group with only the neutral element. Note that in a normal series, each group is a normal subgroup of its immediate predecessor; it does not necessarily follow that G_j is normal in G_k for $k < j - 1$.

Example 3.8. Any finite sequence of descending subgroups, ending with $G_n = 1$, of an abelian group is a normal series. For any group, $G \rhd 1$ is always a (trivial) normal series, and if G is simple, then this is the only normal series. Here are two more interesting examples:

$$S_3 \rhd A_3 \rhd 1, \qquad S_4 \rhd A_4 \rhd H \rhd K \rhd 1, \tag{3.4}$$

where H contains all permutations whose cycle structure consists of two disjoint 2 cycles $(jk)(mn)$, in addition to the identity, and $K = \{1, (12)(34)\}$.

Exercise 3.49. Convince yourself that H is indeed a subgroup, and that $|H| = 4$. Then show that the sequences above are indeed normal series. Also, show that K is not normal in S_4. (Is $H \trianglelefteq S_4$?)

Definition 3.31. A group G is called *solvable* if it has a normal series whose quotient groups G_k/G_{k+1} are all abelian.

Trivially, an abelian group is solvable, but there are many others. In fact, the normal series from the previous example show that both S_3 and S_4 are solvable (later we will see that S_n is not solvable for $n \geq 5$).

Exercise 3.50. Show this. More specifically, verify that all quotients from (3.4) are abelian.

A group of order p^n, p a prime, is called a *p-group.*

Theorem 3.32. *Every p-group G is solvable.*

Proof. By Corollary 3.20, G has a non-trivial center $C \trianglelefteq G$. If $C = G$, then G is abelian and we're done. If not, let $G_1 = C$ and consider the quotient group G/G_1. This is again a p-group, so it has a non-trivial center C_2. By the first isomorphism theorem, $C_2 = G_2/G_1$, where $G_1 \subset G_2 \subseteq G$ and $G_2 \trianglelefteq G$. If $G_2 \neq G$, then we continue in this style and consider the center of the p-group G/G_2 in the next step, which will produce a G_3. Since these groups get larger at each step, we must eventually arrive at $G_n = G$. Now

$$G \rhd G_{n-1} \rhd \ldots \rhd G_1 \rhd 1$$

is a normal series and, by construction, G_k/G_{k-1} is the center of some group and hence abelian. □

In general, suppose we are given some group G and we would like to know whether G is solvable. It is tempting to try to approach this more systematically, as follows. Just to get things started, we need to come up with a normal subgroup K of G, such that G/K is abelian. What do these K's look like? This can be answered neatly if we introduce the *commutator*

$$[a, b] = a^{-1}b^{-1}ab$$

of two elements $a, b \in G$. Notice that $ab = ba$ if and only if $[a, b] = 1$. In particular, a group G is abelian precisely if all commutators are equal to the identity. Moreover, if $\varphi : G \to H$ is a homomorphism, then $\varphi([a, b]) = [\varphi(a), \varphi(b)]$. If we specialize to $H = G/K$ and the natural quotient map here, then this implies that G/K will be abelian precisely if all commutators from G lie in K. In other words, to make the quotient abelian, we must at least divide out all commutators. This motivates:

Definition 3.33. Let G be a group. The *commutator subgroup* or *derived subgroup* G' is defined as the subgroup generated by the commutators $[a, b]$, $a, b \in G$.

Since $[a,b]^{-1} = [b,a]$, we can also describe G' more explicitly as

$$G' = \{[a_1,b_1][a_2,b_2]\dots[a_n,b_n] : n \geq 0, a_j, b_j \in G\}. \tag{3.5}$$

Similarly, if $H \subseteq G$ is a subgroup, then $H' \subseteq G$ is defined as the subgroup that is generated by the commutators $[a,b]$ with $a,b \in H$.

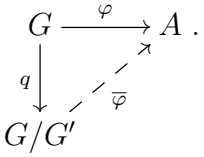
Proposition 3.34. *(a) If $K \trianglelefteq G$, then also $K' \trianglelefteq G$. In particular, $G' \trianglelefteq G$.*
(b) If $K \trianglelefteq G$, then G/K is abelian precisely if $K \supseteq G'$. In particular, G/G' is abelian.

Proof. (a) Observe that $g[a,b]g^{-1} = [gag^{-1}, gbg^{-1}]$. (Since $a \mapsto gag^{-1}$ defines an automorphism, this is actually a special case of an observation made above.) This implies that at least a single commutator $c = [a,b] \in K'$, with $a,b \in K$, has the property that $gcg^{-1} \in K'$ again, for arbitrary $g \in G$. But then (3.5) makes sure that every element $c \in K'$ has this property. So K' is normal, as claimed.

(b) We essentially proved this above: G/K is abelian precisely if all commutators of G lie in K, and this holds precisely if $K \supseteq G'$. (The final claim makes use of the fact that $G' \trianglelefteq G$, which was proved in part (a).) □

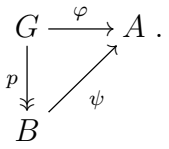
The group G/G' is also called the *abelianization* of G; it is what you obtain when you make G abelian as cheaply as possible (you cannot do this by dividing out less than G'). All this is still named after the Norwegian mathematician *Niels Henrik Abel* (1802–1829); you see that mathematical fame often goes hand in hand with abuse to your name by posterity.

Exercise 3.51. Show that a homomorphism $\varphi : G \to A$ to an *abelian* group A factors through G/G', and the induced homomorphism $\overline{\varphi} : G/G' \to A$ is unique:



Exercise 3.52. Can you also show that G/G' is characterized by the mapping property from the previous Exercise, in the following sense: Suppose that $p : G \to B$ is a surjective homomorphism onto an abelian group B, such that if A is any abelian group and $\varphi : G \to A$ is any homomorphism, then φ factors through B; in more concrete terms,

there is a homomorphism $\psi : B \to A$ so that $\varphi = \psi \circ p$:



Show that then $B \cong G/G'$.

Exercise 3.53. Let H be a subgroup of G with $H \supseteq G'$. Show that $H \trianglelefteq G$.

Exercise 3.54. Let G be a finite group of odd order, and form the product $p = g_1 \dots g_n$ of all elements of G. Show that $p \in G'$.

Exercise 3.55. Let G be a non-abelian group of order p^3, p a prime. Show that then $C = G'$, $|C| = p$, and $G/C \cong \mathbb{Z}_p \times \mathbb{Z}_p$. *Hint:* Make use of the result from Exercise 3.29.

Let's now return to our original project of systematically finding a normal series that establishes that a given group G is solvable, if this is actually true. At the start $G \rhd G_2$ of our normal series, we must choose G_2 such that G/G_2 is abelian, and by Proposition 3.34(b), this means that exactly the normal subgroups $G_2 \supseteq G'$ will work here (and "normal" could be dropped from this sentence, by Exercise 3.53). So perhaps we just want to give $G_2 = G'$ a try? Next, we need a $G_3 \lhd G_2$ such that G_2/G_3 becomes abelian, and again a natural attempt would be $G_3 = G_2' = G''$. We continue in this way; the whole operation will be a success if at some point we reach $G^{(n)} = 1$, and if that doesn't happen, then maybe G wasn't solvable to start with? This impression is correct:

Theorem 3.35. *G is solvable if and only if $G^{(n)} = 1$ for some $n \geq 1$.*

Proof. As we just argued, if $G^{(n)} = 1$, then $G \rhd G' \rhd \dots \rhd G^{(n)} = 1$ is a normal series with abelian quotient groups (which, by the way, has the additional property that each $G^{(k)}$ is normal in the large group G). So G is solvable.

Conversely, assume that G is solvable, and this is witnessed by the normal series

$$G = G_1 \rhd G_2 \rhd G_3 \rhd \dots \rhd G_n = 1.$$

Since the quotients G_k/G_{k+1} are abelian, Proposition 3.34(b) shows that $G_{k+1} \supseteq G_k'$. By applying this observation repeatedly, we see that

$$1 = G_n \supseteq G_{n-1}' \supseteq \left(G_{n-2}'\right)' = G_{n-2}'' \supseteq \dots \supseteq G^{(n-1)},$$

so $G^{(n-1)} = 1$, as claimed. □

Exercise 3.56. Find G' for the dihedral group $G = D_n$. Conclude that D_n is solvable. Can you also determine (that is, find an isomorphic group) the abelianization G/G'; distinguish the cases n even and n odd for this.

Exercise 3.57. Find Q', the abelianization Q/Q', and the center $C(Q)$. Does this remind you of an earlier exercise?

Exercise 3.58. Find $G^{(n)}$, $n \geq 1$, for $G = S_4$.

An interesting general consequence of Theorem 3.35 is:

Theorem 3.36. *(a) Any subgroup and any homomorphic image of a solvable group is solvable.*
(b) If $K \trianglelefteq G$ and both $K, G/K$ are solvable, then so is G.

Proof. (a) If $H \subseteq G$ is a subgroup, then $H^{(k)} \subseteq G^{(k)}$, so the first claim is immediate from Theorem 3.35. As we observed earlier, a homomorphism φ maps commutators $[a,b]$ to commutators $\varphi([a,b]) = [\varphi(a), \varphi(b)]$ again. This implies that $\varphi(G') \subseteq (\varphi(G))'$. On the other hand, every commutator $[x,y]$ of elements $x, y \in \varphi(G)$ is in $\varphi(G')$, by the same formula, so we actually have that $\varphi(G') = (\varphi(G))'$. By iterating this, we obtain that $\varphi(G^{(k)}) = (\varphi(G))^{(k)}$ for arbitrary $k \geq 1$. Now the criterion from Theorem 3.35 gives the claim about homomorphic images.

(b) Let $q : G \to G/K$ be the quotient map. This is surjective, so by what we just discussed, we have that $q(G^{(k)}) = (G/K)^{(k)}$. Since G/K is solvable, $(G/K)^{(n)} = 1$ for large enough n, so $G^{(n)} \subseteq K$. Now K is solvable, too, so $K^{(m)} = 1$ for suitable m, and thus $G^{(m+n)} = 1$ as well, as required. □

Exercise 3.59. Use Theorem 3.36(b) to give a new proof that D_n is solvable.

Exercise 3.60. Let G, H be solvable groups. Show that any semidirect product $G \rtimes H$ is solvable.

Exercise 3.61. Show that all groups of order ≤ 11 are solvable (or, if feeling more ambitious, do it for groups of order ≤ 19; in fact, the smallest non-solvable group is A_5, which has order $5!/2 = 60$).

Theorem 3.37. *A_n is simple for $n \geq 5$.*

Recall that a group G is called simple if it has no normal subgroups other than $G, 1$.

Proof. Suppose that $K \trianglelefteq A_n$, $K \neq 1$. We will show that K contains a 3 cycle. This will imply the Theorem, as follows: let's say $(123) \in K$. Recall that

$$\pi(123)\pi^{-1} = (\pi(1)\pi(2)\pi(3)) \tag{3.6}$$

(show it again perhaps); note also that if π is an odd permutation here, then we can replace it by $\pi(45) \in A_n$, and the right-hand side of (3.6) isn't affected. This shows that as soon as $K \trianglelefteq A_n$ contains one 3 cycle, it will contain *all* 3 cycles. You showed in Exercise 2.64(b) that A_n is generated by the 3 cycles, so $K = A_n$.

To show that K indeed contains a 3 cycle, fix a prime p that divides $|K|$, and then choose a $\pi \in K$ with $o(\pi) = p$. Such a π exists because K has a subgroup of order p by Sylow's first theorem, which must be cyclic. Since the order of any permutation is the least common multiple of its cycle lengths, the cycle decomposition of π must consist of $k \geq 1$ cycles of length p each (and 1 cycles, which we ignore). We now distinguish various cases:
(1) $p = 3$, $k = 1$: this says that π is a 3 cycle and we are done.
(2) $p > 3$: let's say $\pi = (12 \dots p) \dots$. Let $\alpha = (123) \in A_n$. Then

$$\pi\alpha\pi^{-1}\alpha^{-1} = (234)(123)^{-1} = (142),$$

by applying (3.6) to the first three factors. Since π, $\alpha\pi^{-1}\alpha^{-1} \in K$, it follows that K contains a 3 cycle.
(3) $p = 3$, $k > 1$: let's say $\pi = (123)(456) \dots$. Let $\alpha = (124)$, and consider again

$$\pi\alpha\pi^{-1}\alpha^{-1} = (235)(124)^{-1} = (14352).$$

This gets us back to case (2).
(4) $p = 2$, $k = 2m \geq 2$, and π fixes some integer: let's say $\pi = (12)(34) \dots$, and $\pi(5) = 5$. Consider

$$\pi(125)\pi^{-1}(125)^{-1} = (215)(125)^{-1} = (125),$$

and again K contains a 3 cycle.
(5) $p = 2$, $k = 2m \geq 2$, and $\pi(j) \neq j$ for all j: a typical π is $\pi = (12)(34)(56) \dots (n-1\ n)$ (this case can only occur if n is even). Then

$$\pi(125)\pi^{-1}(125)^{-1} = (216)(125)^{-1} = (15)(26),$$

and we're back in case (4). □

Exercise 3.62. Is S_n a simple group, too?

Corollary 3.38. *The groups S_n and A_n are solvable if and only if $n = 1, 2, 3, 4$.*

Proof. For $n = 1, 2$, these groups are abelian and thus trivially solvable. The cases $n = 3, 4$ were discussed at the beginning of this section; see Exercise 3.50.

Now let $n \geq 5$. Theorem 3.37 says that the only normal series for A_n is $A_n \rhd 1$, and since $A_n \cong A_n/1$ is not abelian, it follows that A_n is not solvable. Since A_n is a subgroup of S_n, Theorem 3.36(a) shows that S_n cannot be solvable, either. □

Finally, let us take another look at the material of this section from still another slightly different point of view. We now take an approach that is, in a sense, opposite to the one from Theorem 3.35. Rather than dividing out as little as possible, we now make the elements of the normal series as large as possible.

Definition 3.39. Let G be a group. A *composition series* for G is a normal series

$$G = G_1 \rhd G_2 \rhd G_3 \rhd \ldots \rhd G_n = 1 \tag{3.7}$$

with simple quotient groups G_k/G_{k+1}.

By the first isomorphism theorem, the normal subgroups of G_k/G_{k+1} are exactly the groups H/G_{k+1}, with $H \supseteq G_{k+1}$ and H normal in G_k. In other words, G_k/G_{k+1} will be simple precisely if there are no such groups $H \neq G_k, G_{k+1}$. Or, to rephrase this one more time, (3.7) is a composition series precisely if each G_{k+1} is maximal normal in G_k in the sense that if $G_{k+1} \subset H \trianglelefteq G_k$, then $H = G_k$.

Every finite group G has a composition series: take any normal subgroup $K \lhd G$ (take $K = 1$ if all else fails). Either K is already maximal and can be our G_2, or there's a strictly larger normal subgroup, and if this isn't maximal yet, there's a still larger normal subgroup, and so on. Since G is finite, this process has to stop, and we will find a G_2 eventually. Then repeat the whole procedure to find a maximal normal subgroup G_3 of G_2, and continue until $G_n = 1$.

Composition series and the associated quotient groups are not unique, even up to isomorphism. For example,

$$\mathbb{Z}_6 \rhd \{0, 3\} \rhd 1, \qquad \mathbb{Z}_6 \rhd \{0, 2, 4\} \rhd 1$$

are both composition series for $\mathbb{Z}_6$, and the quotients are (isomorphic to) $\mathbb{Z}_3$, $\mathbb{Z}_2$, in this order, in the first case, and they are $\mathbb{Z}_2$, $\mathbb{Z}_3$ in the second case. So in this example, we do obtain the same quotient groups always, but the order in which they appear is not determined in advance. This is in fact the general situation.

Theorem 3.40 (Jordan-Hölder)**.** *Let G be a finite group with the two composition series*

$$G = G_1 \rhd G_2 \rhd G_3 \rhd \ldots \rhd G_m = 1, \tag{3.8}$$

$$G = H_1 \rhd H_2 \rhd H_3 \rhd \ldots \rhd H_n = 1. \tag{3.9}$$

Then $m = n$, and there is a permutation $\pi \in S_{n-1}$ such that $G_k/G_{k+1} \cong H_{\pi(k)}/H_{\pi(k)+1}$ for $k = 1, 2, \ldots, n-1$.

Proof. We will prove this by induction on $|G|$. Everything is of course clear if $|G| = 1$ (or $= 2, 3, 4, 5, 6, 7$, for that matter), so let's move on to the induction step. If $G_2 = H_2$, then we can apply the induction hypothesis to the smaller group G_2: it follows that $m - 1 = n - 1$, plus we can pair off the quotients from G_2/G_3 and H_2/H_3 on. Since also (trivially) $G_1/G_2 \cong H_1/H_2$, we are done in this case.

If $G_2 \neq H_2$, then we consider G_2H_2. This is a normal subgroup of G that contains both G_2 and H_2 and is distinct from these groups because $G_2 \neq H_2$. However, G_2, H_2 were maximal normal, so $G_2H_2 = G$. Now the second isomorphism theorem shows that $G/H_2 \cong G_2/(G_2 \cap H_2)$ and, similarly, $G/G_2 \cong H_2/(G_2 \cap H_2)$. Since G/G_2, G/H_2 are simple, the first isomorphism theorem shows that $K_3 := G_2 \cap H_2$ is maximal normal in both G_2 and H_2 and thus works as the next group in a composition series. In other words, if we tack on a composition series for K_3, then we obtain two new composition series of G:

$$G = G_1 \rhd G_2 \rhd K_3 \rhd \ldots \rhd K_j = 1, \tag{3.10}$$

$$G = H_1 \rhd H_2 \rhd K_3 \rhd \ldots \rhd K_j = 1 \tag{3.11}$$

We already established the claim for a pair of composition series that start the same way, so by comparing these with the original composition series, we obtain that $j = m$, $j = n$, so $m = n$. Moreover, the G_k/G_{k+1}, $k \geq 2$, are the same groups as G_2/K_3, together with the K_k/K_{k+1}, $k \geq 3$, possibly after rearranging. Also, recall that $G_2/K_3 \cong G/H_2$. So the G_k/G_{k+1}, $k \geq 1$, are the same groups as those from this list:

$$G/G_2, G/H_2, K_3/K_4, K_4/K_5, \ldots, K_{n-1}/1 \tag{3.12}$$

So far, we've compared the composition series (3.8) with (3.10). If we now compare (3.9), (3.11) in the same way, we find that the quotient groups H_k/H_{k+1}, $k \geq 1$, are also the ones from (3.12). □

Theorem 3.41. *Let G be a finite group. Then G is solvable if and only if all quotient groups G_k/G_{k+1} from a composition series are cyclic of prime orders.*

By the Jordan-Hölder Theorem, this condition only depends on the group, not on the specific composition series chosen.

Proof. Since cyclic groups are abelian, a group G with such a composition series is certainly solvable. Conversely, if G is solvable, take any composition series of G. We then know that each quotient G_k/G_{k+1}, being a homomorphic image of a subgroup of G, is solvable, too. Moreover, it is simple, and thus also abelian because only abelian simple groups are solvable. The only simple abelian groups are cyclic groups of order p, p a prime. □

Exercise 3.63. Find a composition series of S_4. What do you know about the quotient groups even before getting started?

3.7. **Further exercises.**

Exercise 3.64. (a) Let A be a subset of a finite group G with (strictly) more than $|G|/2$ elements. Show that then $AA = G$.
(b) Show that this can fail in a monoid.

Exercise 3.65. Let $H \subseteq G$ be a subgroup of a finite group G, and let $K \trianglelefteq G$. Suppose that $|K|$ and $[G : H]$ are relatively prime. Show that then $K \subseteq H$.

Exercise 3.66. Prove that a non-abelian group G has an abelian subgroup $A \supsetneq C(G)$.

Exercise 3.67. (a) Show that a group G can not be the union of two proper subgroups (compare Exercise 2.23).
(b) Show that G is a union of three proper subgroups if and only if G has a normal subgroup K such that $G/K \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Exercise 3.68. Find the centralizer $C(\pi)$, $\pi \in S_n$, for $\pi = (12)$ and $\pi = (123\ldots n)$. *Suggestion:* Find $|C(\pi)|$ first.