MATH 25700: Honors Algebra (I)

Course Notes

Pol Gómez Riquelme, Rushabh Mehta

Fall 2018

Contents

Preface

These are our course notes for *Honors Algebra (I)* (MATH 25700) taught at the University of Chicago by Prof. George Boxer in the Fall quarter of 2018.
Please do let us know at `gomezp@uchicago.edu` or `rmehtany@uchicago.edu` if you find any!

1 Mon. 01/10/18 – basic number theory

1.1 Remainders

Theorem 1.1. *$\forall a, b \in \mathbb{Z}$ where $b > 0$, $\exists!\ q, r \in \mathbb{Z}$ such that $0 \leq r < b$ and*

$$a = q \cdot b + r$$

Existence Proof. Consider the largest $q \in \mathbb{Z}$ such that

$$a - q \cdot b \geq 0$$

We know such a largest q exists by the discreteness of the integers. Moreover, this implies that

$$a - (q+1) \cdot b < 0 \rightarrow a - q \cdot b < b$$

If we define $r = a - q \cdot b$, we have shown the existence of q, r with the appropriate conditions. □

Uniqueness Proof. Suppose there existed two distinct $q, q' \in \mathbb{Z}$ such that there were distinct $r, r' \in \mathbb{Z}$ where $0 \leq r, r' < b$ and

$$a = q \cdot b + r$$
$$a = q' \cdot b + r'$$

Then,

$$r - r' = b \cdot (q - q')$$

This implies that $r - r'$ is a multiple of b, which is a contradiction as r, r' range from 0 to $b - 1$. □

Definition 1.2. If $a, b \in \mathbb{Z}$, we call b a **multiple** of a if $\exists m \in \mathbb{Z}$ such that

$$b = a \cdot m$$

This can also be denoted as $a|b$.

Definition 1.3. d is a **common divisor** of a and b if $d|a$ and $d|b$

Definition 1.4. The **greatest common divisor** of a and b, notated as $\gcd(a, b)$, is the largest common divisor of a, b.

Lemma 1.5. *If $a = q \cdot b + r$ where $q, r \in \mathbb{Z}$, then*

$$\gcd(a, b) = \gcd(b, r)$$

Proof. If $d|a$ and $d|b$, then

$$d|a - q \cdot b \rightarrow d|r$$

If $d|b$ and $d|r$, then

$$d|q \cdot b + r \rightarrow d|a$$

Since this is true for all divisors d, it must be true for the greatest common divisor. □

This lemma motivates the **Euclidean Algorithm**, which uses the lemma to find the gcd relatively quickly.

We do so by rewriting $a = q \cdot b + r$ as $r = a - q \cdot b$, and then creating a sequence of remainders r_n as follows:

$$r_0 = a - q_0 \cdot b$$

$$r_n = r_{n-2} - q_{n-1} \cdot r_{n-1}$$

Since we know that $\forall n\ r_n < r_{n-1}$, and by the well ordering of the naturals, this algorithm always converges to 0: the last non-zero r_n is the gcd.

Theorem 1.6. – *Bézout's Identity*
$\forall a, b \in \mathbb{Z},\ \exists x, y \in \mathbb{Z}$ *such that*

$$x \cdot a + y \cdot b = \gcd(a, b)$$

The proof of this theorem requires inverting the Euclidean algorithm.

1.2 Modular Arithmetic

Definition 1.7. $\forall a, b, n \in \mathbb{Z},\ n > 0$, a and b are considered to be **congruent modulo n** if $n|a - b$. This can be written as

$$a \equiv b \mod n$$

Theorem 1.8. *The congruence relation is an equivalence relation.*

Proof.

1. Reflexive:

   $$n|a - a \to n|0$$

   which is true regardless of n.

2. Symmetric: If $n|a - b$, then

   $$\exists m \in \mathbb{Z}\ \ n \cdot m = a - b$$

   Hence,

   $$n \cdot (-m) = b - a \to n|b - a$$

3. Transitive: If $n|a - b$ and $n|b - c$, n is a divisor of their sum, namely $a - c$.

□

Because the congruence relation is an equivalence relation, we know that it separates $\mathbb{Z}$ into equivalence classes. So, we write $\bar{a}$ to denote the equivalence class of $\mathbb{Z}$ in which a belongs. We denote $\mathbb{Z}/n\mathbb{Z}$ as the set of all equivalence classes of $\mathbb{Z}$ modulo n.

It's trivial to show (a good exercise) that $|\mathbb{Z}/n\mathbb{Z}| = n$, and that

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{a} \mid 0 \leq a < n\}$$

We seek to definitione two binary operations (i.e., $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$) on our new equivalence classes. We choose the following definitions

Definition 1.9. 5 We define **addition** on our equivalence classes, denoted by the operator $+$, as

$$\overline{a} + \overline{b} = \overline{a+b}$$

Definition 1.10. We define **multiplication** on our equivalence classes, denoted by the operator $\cdot$, as

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

We need to be careful about these definitions, since we seek to ensure they are **well definitioned**, which means that the result of addition or multiplication doesn't change based on the choice of member of the given equivalence class I choose.

Theorem 1.11. *The definitions presented in definitions 5 and 6 are well defined.*

Proof. Let us choose two arbitrary members of $\mathbb{Z}/n\mathbb{Z}$, i.e., $\overline{r_1}, \overline{r_2}$ such that $0 \leq r_1, r_2 < n$, and two integers a, b such that $a \in \overline{r_1}$ and $b \in \overline{r_2}$. So, $\exists p, q \in \mathbb{Z}$ such that

$$a = p \cdot n + r_1$$

$$b = q \cdot n + r_2$$

So,

$$a + b = (p+q) \cdot n + (r_1 + r_2) \rightarrow a + b \in \overline{r_1 + r_2}$$

Since r_1, r_2 are not dependent on our choice of a, b, we have proved addition is well defined. Likewise,

$$a \cdot b = n \cdot (pqn + p \cdot r_2 + q \cdot r_1) + r_1 \cdot r_2 \rightarrow a \cdot b \in \overline{r_1 \cdot r_2}$$

which by the same logic proves multiplication is well defined. □

Example. We take the example of $n = 3$, and look at the results of multiplying and adding different classes of $\mathbb{Z}/n\mathbb{Z}$

.

Multiplication

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

Addition

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

□

Definition 1.12. 7 We say that $x \in \mathbb{Z}/n\mathbb{Z}$ is a **unit** or is **invertible** if it has a multiplicative inverse, i.e., $\exists y \in \mathbb{Z}/n\mathbb{Z}$ such that

$$x \cdot y = \overline{1}$$

We denote the subset of invertible elements of $\mathbb{Z}/n\mathbb{Z}$ as $(\mathbb{Z}/n\mathbb{Z})^\times$ (pronounced **crossed**). A neat observation we make is the following:

Theorem 1.13. *5 If $a, n \in \mathbb{Z},\ n > 0$ and $\gcd(a, n) = 1$, then $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ is a unit.*

Proof. By Bézout's Identity,

$$x \cdot a + y \cdot n = 1$$

Hence,

$$\overline{x} \cdot \overline{a} = \overline{1}$$

□

This means that for arbitrary prime p,

$$\mathbb{Z}/p\mathbb{Z} = (\mathbb{Z}/p\mathbb{Z})^{\times}$$

2 Wed. 03/10/18 – symmetries

2.1 Symmetries of an equilateral triangle

An equilateral triangle with 3 vertices has two types of symmetries: *reflections* (S_1, S_2, S_3) and *rotations* (R_1, R_2). We can compose two symmetries to get a third, but in general this operation does not commute: CCW rotation before vertical reflection is *not* equivalent to vertical reflection before CCW rotation, i.e. $S_2 \circ R_1 \neq R_1 \circ S_2$

We can form a table of all possible symmetry compositions:

	id	R_1	R_2	S_1	S_2	S_3
id	id	R_1	R_2	S_1	S_2	S_3
R_1	R_1	R_2	id	S_3	$\cdots$	
R_2	R_2	id	R_1			
S_1	S_1	S_2				
S_2	S_2	$\cdots$				
S_3	S_3					

This example encapsulates the intuition behind the general idea of a group.

Definition 2.1. A **group** is a set G together with a binary operation $\star : G \times G \to G$ such that the following properties hold:

1. (Identity) There is some $e \in G$ such that $e \star g = g \star e = e$.
2. (Inverses) For each $g \in G$ there is some $h \in G$ such that $g \star h = h \star g = e$.
3. (Associativity) For all $g, h, k \in G$ we have $(g \star h) \star k = g \star (h \star k)$.

Note that in general, we do not require commutativity.

Definition 2.2. A group $(G, \star)$ is **Abelian** (or **commutative**) if its group operation $\star$ is commutative.

Examples;

- $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{Z}/n\mathbb{Z}, +)$.
- The counter-example $(\mathbb{Q}, \cdot)$, for 0 has no inverse.
- $(\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}, \cdot)$.
- $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$.
- The *general linear group* $\mathrm{GL}_n(\mathbb{R}) := \{n \times n$ invertible matrices with coefficients in $\mathbb{R}\}$.
- The *special linear group* $\mathrm{SL}_n(\mathbb{R}) := \{n \times n$ matrices with determinant 1 and coefficients in $\mathbb{R}\}$.
- *Dihedral groups* $\mathrm{D}_{2n} :=$ { symmetries of the regular n-gon }.
- *Symmetric groups* (aka *permutation groups*). For any given set X, form $S_X = \{f : X \to X$ a bijection$\}$. If $|X| = n$, we write $S_X = S_n$. Note that $|S_n| = n!$.

Definition 2.3. The **order** of a group $(G, \star)$ is the cardinality of G as a set, i.e. $|G|$. We write $\mathrm{ord}(G)$.

Definition 2.4. An **isomorphism** between two groups $(G, \star_G)$ and $(H, \star_H)$ is a bijection $f : G \to H$ compatible with group structure, i.e. for which

$$f(g_1 \star_G g_2) = f(g_1) \star_H f(g_2).$$

For example, $(\mathbb{Z}/2\mathbb{Z}, +)$ and $((\mathbb{Z}/3\mathbb{Z})^\times, \cdot)$ are isomorphic. In fact, any group of order 2 is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

3 Fri. 05/10/18 – order and subgroups

Theorem 3.1. *The identity element of a group $(G, \cdot)$ is always unique.*

Proof. Suppose not. Let $i, j \in G$ be distinct identity elements. Then, by nature of the identity,

$$i \cdot j = i = j$$

This is a contradiction. □

Theorem 3.2. *For any given element $a \in G$, the inverse of a is unique.*

Proof. Suppose not. Let $i, j \in G$ be distinct inverses to $a \in G$. Then, by properties of the inverse,

$$(i \cdot a) \cdot j = j = i \cdot (a \cdot j) = i$$

This is a contradiction. □

3.1 Notation

In order to make certain group operations more intuitive, we will usually adapt notation from a common group operand, multiplication, to apply to many groups.

1. The group operator applied to elements a, b will be denoted as $a \cdot b$ or simply ab
2. The identity of the group will be denoted 1
3. The inverse element of a will be denoted a^{-1}
4. For $n \in \mathbb{N}$, we will use a^n as shorthand for $a \cdot a \cdot ...a$ with n a's, while a^{-n} will be used as shorthand for $a^{-1} \cdot a^{-1} \cdot ... \cdot a^{-1}$.

For many groups, this notation is quite handy, since many group properties mimic those of multiplication, i.e.,

$$a^{n+m} = a^n \cdot a^m$$
$$(a^n)^m = a^{nm}$$

However, it's important to be careful, as not all properties of multiplication necessarily carry over to group operations. For example, unless the group is Abelian, the following equality does **NOT** always hold:

$$(ab)^n = a^n b^n$$

Occasionally, addition serves as a better parallel to the group operator than multiplication. This is true in groups like $\mathbb{Z}/n\mathbb{Z}$. In these cases, we adopt a slightly different set of notation.

1. The group operator applied to elements a, b will be denoted as $a + b$
2. The identity of the group will be denoted 0
3. The inverse element of a will be denoted $-a$
4. For $n \in \mathbb{N}$, we will use $n \cdot a$ as shorthand for $a + a + ...a$ with n a's, while $(-n) \cdot a$ will be used as shorthand for $-a + -a + ... - a$.

3.2 Order and Subgroups

Definition 3.3. The **order** of an element of a group $a \in G$ is defined as

$$\min\{n \mid a^n = 1\}$$

When the above set is empty, we consider the order of the element to be ∞. We will notate the order of element a as $\text{ord}(a)$

Examples 3.4. In our equilateral triangle group, $\text{ord}(R_1) = 3$ since it takes three unit rotations to return to the original triangle orientation.

Theorem 3.5. *Given a group G, $\forall a \in G$, $\text{ord}(a) \leq |G|$*

Proof. Suppose $\exists a \in G$ such that $\text{ord}(a) > |G|$. Then by the pigeonhole principle, $\exists n, m \in \mathbb{N}$ such that $0 \leq n, m < |G|$, $n \neq m$ and $a^n = a^m$. This means that $a^{|m-n|} = 1$, and $0 < |m - n| < |G|$. This implies that $\text{ord}(a) < |G|$, a contradiction. □

Theorem 3.6. *If $\gcd(a, n) = 1$, and $\varphi(x)$ represents $|\mathbb{Z}/x\mathbb{Z}|$, then*

$$a^{\varphi(n)} \equiv 1 \mod n$$

Proof. This is shown in homework 1. □

Theorem 3.7. *In an arbitrary group G and $a \in G$*

$$\text{ord}(a)|n \iff a^n = 1$$

Proof.
($\Longrightarrow$): $a^n = (a^{\text{ord}(a)})^k = 1^k = 1$
($\Longleftarrow$): $n = \text{ord}(a) \cdot k + r \rightarrow a^n = (a^{\text{ord}(a)})^k \cdot a^r = a^r$.
Hence, $a^r = 1$, which implies $r = 0$. □

Definition 3.8. For a group $(G, \star)$, a set $H \subset G$ is a **subgroup** denoted by $(H, \star)$ if and only if

1. $1 \in H$
2. $\forall a \in H, \;\; a^{-1} \in H$
3. $\forall a, b \in H, \;\; a \star b \in H$

The following examples are of subgroups in groups we have already seen in the course

1. The rotations and the identity operation in the equilateral triangle group explored in section 2.1 is a subgroup.
2. The even integers in the group $(\mathbb{Z}, +)$ is a subgroup.

Theorem 3.9.

$$(H, \star) \textit{ is a subgroup of } (G, \star) \iff \forall a, b \in H, \;\; a \star b^{-1} \in H$$

Proof.
($\Longrightarrow$) : This is true by properties 2 and 3 of subgroups.
($\Longleftarrow$) :

1. If $a = b$, we know that $a \star a^{-1} = 1 \in H$.
2. Since $1 \in H$, $\forall b \in H$, $\ 1 \star b^{-1} = b^{-1} \in H$.
3. $\forall a, b \in H$, we know that $b^{-1} \in H$, so $a \star (b^{-1})^{-1} = a \star b \in H$.

□

Definition 3.10. Given two groups $(G_1, \star_1)$ and $(G_2, \star_2)$, the **direct product** of the groups, denoted by $(G_1 \times G_2, \star_{12})$, is defined as the cartesian product of the sets G_1, G_2, and the operation

$$(a_1, b_1) \star_{12} (a_2, b_2) = (a_1 \star_1 b_1, a_2 \star_2 b_2)$$

As an exercise, try to prove that this definition guarantees that the direct product of two groups will be a group.

4 Mon. 08/10/18 – homomorphisms and the cyclic groups

Helpful homework tip; given a group G and arbitrary $a, b \in G$,

- $ax = b$ has a unique solution, namely $x = a^{-1}b \in G$; and
- $xa = b$ has a unique solution, namely $x = ba^{-1} \in G$.

Think of fixing an element a in the column of the group multiplication table; every single $b \in G$ can be obtained by a unique expression ax for some $x \in G$. In other words, every row in the multiplication table must be a permutation of G. The same argument applies for columns. This is referred to as the *Sudoku rule*.

Another argument to see why; if we had two distinct elements $x, y \in G$ for which $ax = ay$, this would immediately imply $a^{-1}ax = a^{-1}ay$ and so $x = y$.

4.1 Homomorphisms, kernels

Definition 4.1. Given groups G, H, a function $f : G \to H$ is a **homomorphism** if for all $a, b \in G$ we have

$$f(ab) = f(a)f(b).$$

(Hence, an *isomorphism* is a bijective homomorphism.)
Examples;

- The map $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ sending $a \in \mathbb{Z}$ to its equivalence class $\overline{a}$ modulo n.
- The map $\mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$ sending a matrix A to its determinant $\det(A)$.

Proposition 4.2. *If $f : G \to H$ is a homomorphism, then $f(1) = 1$ and $f(x^{-1}) = f(x)^{-1}$.*

Proof. First, we have $f(1) = f(1 \cdot 1) = f(1)f(1)$, so $1 = f(1)$.
Furthermore, $1 = f(1) = f(xx^{-1}) = f(x)f(x^{-1})$, so $f(x)^{-1} = f(x^{-1})$. □

Proposition 4.3. *Let $f : G \to H$ be a homomorphism, and fix $a \in G$. If a has finite order, then so does $f(a)$, in particular it holds that*

$$\mathrm{ord}(f(a)) \mid \mathrm{ord}(a).$$

Proof. We have $a^{\mathrm{ord}(a)} = 1$, so $f(a^{\mathrm{ord}(a)}) = 1$ and so $f(a)^{\mathrm{ord}(a)} = 1$, which by (??) implies that $\mathrm{ord}(f(a)) \mid \mathrm{ord}(a)$. □

Definition 4.4. If $f : G \to H$ is a homomorphism, we define its **kernel** by

$$\ker(f) = \{a \in G \mid f(a) = 1\}.$$

Proposition 4.5. $\ker(f)$ *is a subgroup of G, and* $\mathrm{im}(f)$ *is a subgroup of H.*

Proof. Let $a, b \in \ker(f)$. Then $f(ab^{-1}) = f(a)f(b)^{-1} = 1$, so $ab^{-1} \in \ker(f)$. By the subgroup criterion, we get that $\ker(f)$ is a subgroup of G.

Let $x, y \in \text{im}(f)$. Then there exist $a, b \in G$ such that $f(a) = x$ and $f(b) = y$. It is clear that $ab \in G$, and furthermore $f(ab) = f(a)f(b) = xy$, so $xy \in \text{im}(f)$. Again by the subgroup criterion, we conclude that $\text{im}(f)$ is a subgroup of H. □

Proposition 4.6. *Let $f : G \to H$ be a homomorphism; f is injective $\iff$ f has trivial kernel.*

Proof. ($\Longleftarrow$) With $\ker(f) = \{1\}$, assume there exists a pair $a, b \in G$ such that $f(a) = f(b)$. Then $f(a)f(b)^{-1} = 1$, so $f(ab^{-1}) = 1$, that is, $ab^{-1} \in \ker(f)$, but necessarily $ab^{-1} = 1$ so $a = b$.

($\Longrightarrow$) Let $a \in \ker(f)$. We have $f(a) = 1 = f(1)$, but f is injective, so $a = 1$. □

4.2 Cyclic groups

Definition 4.7. A group G is **cyclic with generator** $a \in G$ if every element of G is of the form a^n for some $n \in \mathbb{Z}$.

(Note that cyclic groups are automatically Abelian, for $a^n a^m = a^{n+m} = a^{m+n} = a^m a^n$.)
Examples;

- $\mathbb{Z}/n\mathbb{Z}$ with generator 1;
- $\mathbb{Z}$ with generator 1.

Theorem 4.8. *Let G be a cyclic group with generator $g \in G$. The following statements hold:*

1. *If g has infinite order, then the map $f : \mathbb{Z} \to G$ given by $n \mapsto g^n$ is an isomorphism; and*
2. *If g has order $k < \infty$, then the map $f : \mathbb{Z}/k\mathbb{Z} \to G$ given by $\overline{n} \mapsto g^n$ is a well-defined isomorphism.*

Proof. 1. First of all, f is indeed a homomorphism, for $f(n + m) = g^{n+m} = g^n g^m = f(n)f(m)$. Furthermore, its kernel is trivial, for if there is some $n \neq 0$ in the kernel, WLOG $n > 0$ (we can just take the inverse and it must lie in the kernel still), then $g^n = e$ but this contradicts the infite order of g. Finally, f is surjective, since

$$\text{im}(f) = \{g^n \mid n \in \mathbb{Z}\} = G,$$

by G being cyclic with generator g.

□

5 Wed. 10/10/18 – Cyclic and Modulo Groups

5.1 Generators

Definition 5.1. Let $(G, \star)$ be a group, and $g \in G$. The **cyclic subgroup generated by g**, denoted by $\langle g \rangle$, is

$$\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$$

Theorem 5.2.

$$|\langle g \rangle| = \text{ord}(g)$$

Proof. This is left as an exercise to the reader. □

We note that if $\text{ord}(g)$ is finite,

$$\langle g \rangle = \{1, g, g^2, ..., g^{n-1}\}$$

If $\text{ord}\, g = |G|$, it's pretty obvious that $\langle g \rangle = G$ and G is a cyclic group generated by g. We call g the **generator** of G.

Theorem 5.3. *Let G be a cyclic group with generator g.*

1. *All subgroups of G are cyclic.*
2. *If $|G| = \infty$, all subgroups of G are of the form $\langle g^k \rangle$, $k > 0$.*
3. *If $k \in \mathbb{Z}$, $|\langle g^k \rangle| = |\langle g^{\gcd(k,n)} \rangle|$*
4. *If $|G| = n \in \mathbb{N}$, all subgroups of G can be expressed as $\langle g^d \rangle$, $d|n$. $|\langle g^d \rangle| = \frac{n}{d}$.*

Proof.

1. Let G = $\langle g \rangle$. Let H be a subgroup of G. Define $k \in \mathbb{N}$ as

   $$k = \inf\{i > 0 \mid g^i \in H\}$$

   We now seek to show that $H = \langle g^k \rangle$.

   If $g^m \in H$, then we can decompose $m = q \cdot k + r$ where $0 \leq r < k$. This implies that

   $$g^m = (g^k)^q \cdot g^r \to g^r = g^m \cdot (g^k)^{-q}$$

   We know by the properties of group operations that $g^m \cdot (g^k)^{-q} \in H$, so $g^r \in H$. By the properties of infimum, $r = 0$. Hence, $g^m \in \langle g^k \rangle$. On the other hand, $\forall g^m \in \langle g^k \rangle$, $g^m \in H$ since the subgroup has to be closed over the operation.

   This implies $H = \langle g^k \rangle$, so H is cyclic.
2. This follows directly from the result in 1 since for all subgroups H of G, H must be generated by an element, and every element of G is of the form g^k for some $k > 0$.
3. Since $\gcd(n, k) \mid k$, $\langle g^k \rangle \subseteq \langle g^{\gcd(n,k)} \rangle$. By Beźout's Identity, $\exists x, y \in \mathbb{Z}$

   $$\gcd(n, k) = xn + yk$$

   Hence,

   $$g^{\gcd(n,k)} = (g^n)^x \cdot (g^k)^y = (g^k)^y \in \langle g^k \rangle$$

4. We know that $(g^d)^{n/d} = g^n = 1$, and if $0 < k < n/d$, $(g^d)^k \neq 1$ since then, $g^{dk} = 1 \to |G| < n$.

□

Theorem 5.4. *If g is a generator for cyclic group G such that $|G| = \infty$, g^{-1} is also a generator for G, and there are no other generators. If $|G| = n$, the generators of G are elements of the form g^k where $\gcd(n, k) = 1$.*

Proof. If $|G| = \infty$, we know that $\langle g \rangle = \langle g^{-1} \rangle$ since $\forall m \in \mathbb{Z}$, $g^m = (g^{-1})^{-m}$. There are no other generators, since we know that if $\langle a \rangle = \langle b \rangle$, $\exists n, m \in \mathbb{Z}$ such that $a = b^n$, $b = a^m$. So, $a = a^{nm} \to nm = 1$. This means that a and b are inverses, so we are done.

If $|G| = n$, this is obvious by Beźout's. □

Theorem 5.5. *If G is cyclic with generator g, and $|G| = n$,*

$$\operatorname{ord}(g^k) = \frac{n}{\gcd(n, k)}$$

Proof.

$$\operatorname{ord}(g^k) = |\langle g^k \rangle| = |\langle g^{\gcd(n,k)} \rangle| = \frac{n}{\gcd(n, k)}$$

□

Theorem 5.5 directly implies that for prime p, $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p - 1$.

5.2 Chinese Remainder Theorem

If $n, m > 0$, and $n \mid m$, we can define a homomorphism

$$\begin{aligned} \phi : \mathbb{Z}/m\mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z} \\ k \pmod m &\mapsto k \pmod n \end{aligned}$$

Proving that this homomorphism is well-defined is left as an exercise to the reader.

Theorem 5.6. *If $n, m \in \mathbb{N}$, $\gcd(n, m) = 1$, the mapping*

$$\begin{aligned} \phi : \mathbb{Z}/mn\mathbb{Z} &\to (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}) \\ k \pmod{mn} &\mapsto (k \pmod m,\ k \pmod n) \end{aligned}$$

is an isomorphism.

Proof. It's trivial to show that this mapping is a well-defined homomorphism, and that

$$|\mathbb{Z}/mn\mathbb{Z}| = |(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})|$$

So, we need to show that this mapping is either injective or surjective. We will show that the mapping is surjective.

Let $(a \pmod m, b \pmod n)$ be an arbitrary element of $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$. By Beźout's Identity, we can find $x, y \in \mathbb{Z}$ such that

$$mx + ny = 1$$

So,

$$ny \equiv 1 \pmod m$$
$$mx \equiv 1 \pmod n$$

Let $k = any + bmx$. We've shown that $f(k) = (a \pmod m, b \pmod n)$. $\square$

6 Fri. 12/10/18 – symmetric groups

Recall that for any given set X we form the symmetric group $S_X := \{f : X \to X \text{ bijection }\}$ under function composition.

Proposition 6.1. *If $g : X \to Y$ is a bijection of sets, then the map $\phi : S_X \to S_Y$ given by $f \mapsto g \circ f \circ g^{-1}$ is an isomorphism of groups.*

Proof. Consider the following diagram:

$$\begin{array}{ccc} X & \xrightarrow{g} & Y \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle ?} \\ X & \xrightarrow{g} & Y \end{array}.$$

We claim that $f \mapsto g \circ f \circ g^{-1}$ is an isomorphism when S_x and S_y (trace the path on the diagram with your finger).

First, take two bijections $f, f' : X \to X$, and we have

$$(g \circ f \circ g^{-1}) \circ (g \circ f' \circ g^{-1}) = g \circ f \circ f' \circ g^{-1} = g \circ (f \circ f') \circ g^{-1}.$$

Hence ϕ does define a homomorphism. It is furthermore bijective, since the map $h \mapsto g^{-1} \circ h \circ g$ is its inverse.

□

It follows that when $|X| = n$, we write $S_X \simeq S_n = S_{\{1,2,\ldots,n\}}$. In general, we consider the latter canonical.

6.1 Cycles

We write permutations $\sigma \in S_n$ as

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

This form is, however, not super useful for understanding permutations. Consider the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 1 & 5 & 2 \end{pmatrix}.$$

Starting at 1 and repeatedly applying our permutation, we discover a loop $1 \to 3 \to 4 \to 1$ of length 3, starting at 2 we get $2 \to 6 \to 2$ of length 2, and starting at 5 we simply get $5 \to 5$. Note that these loops cover all elements of our permutation. We can readily argue what the order of σ is: applying it a multiple of 3 times we get 1 back to 1; we also need to get 2 back to 2, which only happens when we apply the permutation an even number of times. Hence, we see that $\text{ord}(\sigma) = 3 \cdot 2 \cdot 1 = 6$.

Definition 6.2. An m-**cycle** $(a_1 a_2 \cdots a_m) \in S_n$, where $a_i \in \{1, 2, \ldots, n\}$ are distinct, is the permutation

$$\sigma(x) = \begin{cases} x & \text{if } x \notin \{a_1, \ldots, a_m\} \\ a_{i+1} & \text{if } x = a_i, 1 \leq i < m \\ a_1 & \text{if } x = a_m. \end{cases}$$

It is clear that an m-cycle has order m, for it defines a loop $a_1 \to a_2 \to \cdots \to a_m \to a_1$.

We say two cycles $\sigma = (a_1 a_2 \cdots a_m)$ and $\tau = (b_1 b_2 \cdots b_k$ are **disjoint** if $\{a_1, \ldots, a_m\} \cap \{b_1, \ldots, b_k\} = \emptyset$. Then $\sigma\tau = \tau\sigma$, i.e. disjoint cycles commute.

An expression of $\sigma \in S_n$ of the form $\sigma = \tau_1 \cdots \tau_k$, with τ_i pairwise disjoint cycles, is called a **cycle decomposition** of σ.

Under the two following identifications, we will show that cycle decompositions *exist* for all $\sigma \in S_n$, and that furthermore they are *unique*.

- The cycles $(a_1 a_2 \cdots a_m)$, $(a_2 a_3 \cdots a_m a_1)$, and in general $(a_k \cdots a_m a_1 \cdots a_{k-1})$ are considered to be equivalent;
- We do not write 1-cycles (a 1-cycle is just the identity).

Theorem 6.3 (Cycle decomposition)**.** *If $\sigma \in S_n$, then σ admits a cycle decomposition, which is moreover unique up to reordering and removing 1-cycles.*

The following concept will be extremely useful:

Definition 6.4. Let X be a set, and fix $\sigma \in S_X$. We say that $x, y \in X$ are in the same **orbit** if $x = \sigma^i(y)$ for some $i \in \mathbb{Z}$.

The orbits of a permutation define an equivalence relation on X; equivalence classes are orbits.

Proof of Existence. Let $C_1, \ldots, C_k$ be the orbits of σ on $\{1, 2, \ldots, n\}$. Pick an element $x_{i,1} \in C_i$ for each $i = 1, \ldots, k$, i.e. an element of each orbit. Let m_i be the smallest positive integer for which $\sigma^m(x_{i,1}) = x_{i,1}$, and let $x_{i,j} = \sigma^{j-1}(x_{i,1})$ for $i = 1, \ldots, k$, $j = 1, \ldots, m_i$. Then

$$\sigma = (x_{1,1} x_{1,2} \cdots x_{1,m_1}) \cdots (x_{k,1} x_{k,2} \cdots x_{k,m_k}).$$

□

Proof of Uniqueness. If $\sigma = (x_{1,1} x_{1,2} \cdots x_{1,m_1}) \cdots (x_{k,1} x_{k,2} \cdots x_{k,m_k})$ is a product of disjoint cycles, its orbits are exactly $C_1 = \{x_{1,1}, x_{1,2} \ldots, x_{1,m_1}\}, \ldots, C_k = \{x_{k,1}, x_{k,2} \ldots, x_{k,m_k}\}$. Any other product of disjoint cycles corresponding to these orbits are equivalent by our previous two considerations. □

6.2 Transpositions

Definition 6.5. A 2-cycle is called a **transposition**.

(However, not all permutations of order 2 are transpositions.)

Theorem 6.6. *The group S_n is generated by transpositions.*

This is fundamentally the same as, given a list of indexed cards in a random order, claiming that *we can bring the cards back to their original order by repeatedly swapping pairs with our hands*, which better be true.

Proof. It suffices to show that any m-cycle $(a_1 \cdots a_m)$ is a product of transpositions, by our cycle decomposition theorem. For this, note that

$$(a_1 \cdots a_m) = (a_1 a_m)(a_1 a_{m-1}) \cdots (a_1 a_3)(a_1 a_2),$$

giving a total of $m - 1$ transpositions (** some note on how to remember this which i can't read from my notes **). □

Theorem 6.7. *Given $\sigma \in S_n$, if we write $\sigma = s_1 \cdots s_k = t_1 \cdots t_l$ with s_i and t_i transpositions, then $k \equiv l \pmod 2$.*

Proof. Next time. □

Definition 6.8. We say that $\sigma \in S_n$ is an **even permutation** if it is the product of an even number of transpositions; else, it is an **odd permutation**.

Warning! If m is even, an m-cycle is *odd*; and if m is odd, an m-cycle is *even* (because of our previous remark in Theorem 6.6).

7 Mon. 15/10/18 – Subgroups of the Symmetric Group

Recall Theorem 6.7 (now 7.1) from last class:

Theorem 7.1. *Given $\sigma \in S_n$, if we write $\sigma = s_1 \cdots s_k = t_1 \cdots t_l$ with s_i and t_i transpositions, then $k \equiv l \pmod 2$.*

We will present a combinatorial proof of this theorem. In order to do so, we define

Definition 7.2. For $\sigma \in S_n$, we define the **length** of σ, denoted as $l(\sigma)$, to be

$$l(\sigma) = |\{(i,j) \mid 1 \leq i < j \leq n,\ \sigma(i) > \sigma(j)\}|$$

We now can prove Theorem 7.1

Proof. Notice that the theorem is equivalent to the claim that $\forall s$ transpositions,

$$l(\sigma \cdot s) \equiv l(\sigma) + 1 \pmod 2$$

Let $s = (i\ j)$ (WLOG $i < j$). Then, by definition, $\sigma \cdot s(i) = \sigma(j),\ \sigma \cdot s(j) = \sigma(i)$ and for all other x, $\sigma \cdot s(x) = \sigma(x)$.

In pictorial form,

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & i & \cdots & j & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(i) & \cdots & \sigma(j) & \cdots & \sigma(n) \end{pmatrix}$$

$$\sigma \cdot s = \begin{pmatrix} 1 & 2 & \cdots & i & \cdots & j & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(j) & \cdots & \sigma(i) & \cdots & \sigma(n) \end{pmatrix}$$

Now consider $1 \leq a < b \leq n$. We seek to see whether $(a\ b) \in l(\sigma),\ l(\sigma \cdot s)$. This is left as an exercise for the reader.

□

8 Wed. 17/10/18 – last word on permutations, general congruences

8.1 More on the order of permutations

Proposition 8.1. *Given $\sigma \in S_n$, the following statements hold:*

1. *The order of σ is the least common multiple of the lengths of the cycles of σ.*
2. *σ is even $\iff$ the number of even-length cycles of σ is even.*

Proof (1). If σ, τ are disjoint permutations, then $\langle\sigma\rangle \cap \langle\tau\rangle = \{1\}$. By HW#2, we get $\mathrm{ord}(\sigma\tau) = \mathrm{lcm}(\mathrm{ord}(\sigma), \mathrm{ord}(\tau))$. The proposition follows by induction. □

Proof (2). Remember that an m-cycle is even $\iff$ m is odd.

Hence, if $\sigma = \sigma_1 \cdots \sigma_k$ is the cycle decomposition of σ, we have that σ is even $\iff$ it has an even number of odd cycles $\iff$ it has an even number of even-length cycles. □

8.2 Congruences on abstract groups

We want to generalize the notion of "congruence" from the integers to abstract groups. The usual setup is, given $a, b \in \mathbb{Z}$ and $n > 0$, we say $a \equiv b \pmod{n}$, read "a is equivalent to b modulo n" iff $b = a + kn$.

From this, we define the congruence class of any $a \in \mathbb{Z}$ by $\overline{a} = a + n\mathbb{Z} = \{a + nk \mid k \in \mathbb{Z}\}$. The goal is to replace $\mathbb{Z}$ with any group G, and $n\mathbb{Z}$ with an arbitrary subgroup $H \subset G$.

In fact, we can already do this. We only need be aware that multiplication in a group is *not* commutative in general, which gives rise to two distinct equivalence relations (in principle).

Fix a group G and a subgroup $H \subset G$. We say that $a \overset{l}{\sim} b$, i.e. "a is left-equivalent to b modulo H" $\iff$ $a = bh$ for some $h \in H$, and similarly $a \overset{r}{\sim} b$, i.e. "a is right-equivalent to b modulo H" $\iff$ $a = hb$ for some $h \in H$.

Note; (again) if G is abelian, the two relations coincide.

We also note that, with $G = \mathbb{Z}$ and $H = n\mathbb{Z}$, these two notions of congruence reduce to usual congruence in $\mathbb{Z}$ modulo n.

Proposition 8.2. $\overset{l}{\sim}$ *is an equivalence relation.*

Proof. Reflexivity: we have $a = a \cdot 1$, and $1 \in H$.

Symmetry: given $a \overset{l}{\sim} b$, we have $a = bh$, so $ah^{-1} = b$ with $h^{-1} \in H$, hence $b \overset{l}{\sim} a$.

Transitivity: given $a \overset{l}{\sim} b$ and $b \overset{l}{\sim} c$, we have $a = bh$ and $b = ch'$, so $a = c(h'h)$ with $h'h \in H$, thus $a \overset{l}{\sim} c$. □

From this, we can immediately consider the equivalence class of any $a \in G$: we write it as

$$\{b \in G \mid b \overset{l}{\sim} a\} = \{b \in G \mid b = ah, h \in H\} = aH,$$

where $aH = \{ah \mid h \in H\}$. In general,

Definition 8.3. A **left coset** for a subgroup $H \subseteq G$ is a set of the form $aH = \{ah \mid h \in H\}$ for some $a \in G$.

Similarly for **right coset**.

We define the congruence classes of G by $G/H = \{gH \mid g \in G\}$, read "$G$ modulo H", and $H \setminus G = \{Hg \mid g \in G\}$, read "$H$ dom G".[1]

Definition 8.4.

As an example, we compute the right cosets of $H = \langle (12) \rangle$ in S_3:

- $1H = H = \{1, (12)\} = (12)H$,
- $(13)H = \{(13), (13)(12) = (123)\} = (123)H$,
- $(23)H = \{(23), (132)\} = (132)H$.

Similarly, we compute the left cosets:

- $H1 = H = H(12)$,
- $H(13) = H(132)$,
- $H(23) = H(123)$.

Note that, in general *right and left cosets are different!* However, we can relate them nicely:

Theorem 8.5. *There is a bijection $G/H \to H \setminus G$ given by $gH \mapsto Hg^{-1}$.*

Proof. We abuse notation and write

$$\begin{aligned}(gH)^{-1} &= \{(gh)^{-1} \mid h \in H\} \\ &= \{h^{-1}g^{-1} \mid h \in H\} \\ &= \{hg^{-1} \mid h \in H\} = Hg^{-1},\end{aligned}$$

the last equality by the fact that inversion is a bijection from G to itself. Hence $gH \mapsto (gH)^{-1} = Hg^{-1}$ is a bijective map between right and left cosets. □

Definition 8.6. Given a subgroup $H \subseteq G$, we define the **index** of H in G by $[G : H] = |G/H| = |H \setminus G|$.

Theorem 8.7 (Lagrange)**.** *Let G be a finite group, $H \subseteq G$ a subgroup. Then*

$$|G| = |H| \cdot [G : H].$$

Proof. Since G/H splits G into equivalence classes, we have $G = \coprod_{gH \in G/H} gH$, so

$$|G| = \sum_{gH \in G/H} |gH| = \sum_{gH \in G/H} |H| = |H| \cdot [G : H],$$

the penultimate equality from the bijection $H \to gH$ given by $h \mapsto gh$. □

[1] Note that "dom" for $H \setminus G$ is decidedly *not* standard.

9 Fri. 19/10/18 – ?

10 Mon. 22/10/18 – why quotients?

10.1 Simple groups

Some examples of quotient groups:

- Since $A_n \subseteq S_n$ has index 2, it is normal. Hence S_n/A_n is a quotient group, and in particular of the form $A_n/S_n = \{A_n, \{\text{odd perms.}\}\}$.
- $\mathrm{O}(2)$ = group of rotations and reflections in $\mathbb{R}^2$ ("orthogonal group"). Similarly, $\mathrm{SO}(2) \subseteq \mathrm{O}(2)$, the group of rotations, has index 2, i.e. it is normal. Hence $\mathrm{O}(2)/\mathrm{SO}(2) \simeq \mathbb{Z}/2\mathbb{Z}$, it has the same kind of "parity law" as A_n/S_n.
- $G = D_8$, whose center $\mathrm{Z}(\mathrm{D}_8) = \{1, R_\pi\}$ is of course normal. Hence $D_8/\mathrm{Z}(D_8)$ has 4 elements, and is isomorphic to D_4. If $s \in D_8$ is a reflection, then $(s\,\mathrm{Z}(D_8))^2 = \mathrm{Z}(D_8)$ so reflection cosets have order 2, while $r \in D_8$ a rotation by $\pi/2$ in either direction gives $(r\,\mathrm{Z}(D_8))^2 = R_\pi\,\mathrm{Z}(D_8) = \mathrm{Z}(D_8)$ by R_π being in the center, so rotation cosets have order 2 as well. Hence necessarily $D_8/\mathrm{Z}(D_8) \simeq D_4$.
-

Why do we care about quotient groups? If we want to understand G, and have a normal subgroup $H \subseteq G$, understanding H itself and G/H can give us a good glimpse into G.

Definition 10.1. We say that a non-trivial group G is **simple** if the only normal subgroups it contains are $\{1\}$ and G itself.

Ex; with p prime, the group $\mathbb{Z}/p\mathbb{Z}$ is simple. With $n \geq 5$, the group A_n is simple (while A_4 is *not*); this relates to the insolvability of the quintic.

Simple groups are the "building blocks" of all finite groups.

Proposition 10.2. *S_n has no proper normal subgroups of odd index.*

Proof. Suppose $H \subseteq S_n$ were a normal subgroup of odd index. For a transposition $s \in S_n$, we have $sH \in S_n/H$, and $(sH)^2 = H$ but $|S_n/H|$ is odd; hence sH has necessarily order 1, i.e. $s \in H$ in the first place. Since transpositions generate S_n, we have $S_n \subseteq H$ and so H is not a proper subgroup of S_n. □

10.2 Quotients and homomorphisms

Proposition 10.3. *If $f : G \to H$ is a group homomorphism,* $\ker f$ *is normal in G.*

Proof. Fix any $g \in G$, $x \in \ker f$. We have

$$f(gxg^{-1}) = f(g)f(x)f(g)^{-1} = f(g)f(g^{-1}) = 1,$$

so $gxg^{-1} \in \ker f$, i.e. $\ker f$ is normal. □

Definition 10.4. If $H \subseteq G$ is normal, we define the **canonical homomorphism** $f : G \to G/H$ given by $g \mapsto gH$.

Note that this is well defined by normality; (why????). Also notice that $\ker f = H$, since $g \in H$ iff $gH = H$.

We conclude that $N \subseteq G$ is normal $\iff$ N is the kernel of some homomorphism.

Remark; the image of a normal subgroup through a homomorphism need not be normal in the codomain.

10.3 1st Isomorphism Theorem

Theorem 10.5 (1st ISO)**.** *Let $f : G \to H$ be a group homomorphism. Then there exists a well-defined isomorphism*

$$\begin{aligned} \overline{f} : G/\ker f &\to \operatorname{im}(f) \\ a \ker f &\mapsto f(a). \end{aligned}$$

Proof WELL-DEFINED. Take $a' = ax$, $a \in G$, $x \in \ker f$. Then

$$\overline{f}(a' \ker f) = f(a') = f(ax) = f(a)f(x) = f(a).$$

□

Proof HOMOMORPHISM.

$$\begin{aligned} \overline{f}((a \ker f)(b \ker f)) &= \overline{f}(ab \ker f) \\ &= f(ab) = f(a)f(b) = \overline{f}(a \ker f)\overline{f}(b \ker f). \end{aligned}$$

□

Proof BIJECTIVE. If $\overline{f}(a \ker f) = 1$, then $f(a) = 1$, only the case if $a \in \ker f$ so $\ker \overline{f} = 1 \cdot \ker f$. In other words, the kernel of $\overline{f}$ is trivial. □

Note; if $\varphi : G \to H$ is a homomorphism of finite groups, then $|\operatorname{im} \varphi| = |G/\ker \varphi| = \frac{|G|}{|\ker \varphi|}$. Hence $|\operatorname{im} \varphi| \cdot |\ker \varphi| = |G|$, reminiscent of the Rank-Nullity theorem in linear algebra.

The takeaway of the 1st isomorphism theorem is the following: if we want to show $G/N \simeq H$, construct a surjective homomorphism $G \to H$ the kernel of which is N. Hence by the theorem, $G/\ker f \simeq \operatorname{im} f$, i.e. $G/N \simeq H$.

11 Wed. 24/10/18 – isomorphism theorems

12 Fri. 26/10/18 – Midterm I

Problem 1. (10 points) True or false. Write one or two sentences justifying your answer:

(a) There exists a permutation $\sigma \in S_7$ such that $\sigma^2 = (123)(45)(67)$.

Answer. True. Consider $\sigma = (1\,3\,2)(4\,6\,5\,7)$. □

(b) $(\mathbb{Z}/15\mathbb{Z})^\times$ is cyclic.

Answer. False. By the Chinese remainder theorem, we have $(\mathbb{Z}/15\mathbb{Z})^\times \simeq (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times$, with the groups on the right having order 2 and 4 respectively, hence an element of the product having order 4 at most, less than $|\,(\mathbb{Z}/15\mathbb{Z})^\times\,| = 8$. □

(c) Any group of order 9 is cyclic.

Answer. False. Consider $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, which has exactly nine elements but is not cyclic, since any element has order 3 at most. □

(d) There exists a permutation $\sigma \in A_5$ of order 6.

Answer. False. Such a permutation must consist of either a 6-cycle or a 3-cycle and a 2-cycle: 6-cycles do not exist in S_5, and a 3-cycle plus a 2-cycle is odd, hence is not in A_5. □

(e) If H and K are normal subgroups of a group G then $H \cap K$ is also a normal subgroup of G.

Answer. True. Fix $x \in H \cap K$, and let $g \in G$ be arbitrary. Then $gxg^{-1} \in H$ by $r \in H$ and H being normal, and $gxg^{-1} \in K$ for the same reason, so $gxg^{-1} \in H \cap K$. Thus $H \cap K$ is normal in G. □

Problem 2. (10 points)

(a) Using that $3 = 17 \cdot 435 - 11 \cdot 672$ find an integer n satisfying the congruences

$$n \equiv 9 \pmod{435}$$
$$n \equiv 12 \pmod{672}.$$

Solution. □

(b) Consider the permutation $\sigma \in S_{10}$ given by

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 7 & 8 & 1 & 9 & 4 & 5 & 3 & 10 & 6 & 2 \end{pmatrix}.$$

Find its cycle decomposition, its order, and whether it is even or odd.

Solution. By evaluating each index manually, we get $\sigma = (1\,7\,3)(2\,8\,10)(4\,9\,6\,5)$. Its order is $\mathrm{ord}(\sigma) = \mathrm{lcm}(3, 3, 4) = 12$. It contains an odd number of even-length cycles, so it is an odd permutation. □

(c) Let G be a cyclic group of order 99 with generator g. How many elements $x \in G$ are there with $x^{22} = g^{33}$?

Solution. Note that if x and y are two solutions to the equation, then $(xy^{-1})^{22} = 1$, and conversely if $z^{22} = 1$, then $(xz)^{22}$ is also a solution. Hence counting solutions to $x^{22} = g^{33}$ is equivalent to counting solutions to $x^{22} = 1$. Note that $\gcd(22, 99) = 11$, so x is a solution iff $x^{11} = 1$, whence (...). □

Problem 3. (5 points) Let G and H be finite groups with $(|G|, |H|) = 1$. Show that any homomorphism $f : G \to H$ must be trivial (i.e. $f(g) = 1$ for all $g \in G$).

Proof. Fix $g \in G$. We have that $\text{ord}(g) \mid |G|$, and by homomorphism properties we also have $\text{ord}(f(g)) \mid \text{ord}(g)$, whence $\text{ord}(f(g)) \mid |G|$ and since $\text{ord}(f(g)) \mid |H|$ too, we have the contradiction $(|G|, |H|) > 1$, unless $f(g) = 1$. □

Problem 4. (5 points) Prove that no subgroup of S_6 is isomorphic to $S_3 \times S_4$.

Proof. We argue by considering the order of a carefully chosen element in $S_3 \times S_4$, namely $\sigma = ((1\,2\,3), (1\,2\,3\,4))$. Note that $\text{ord}((1\,2\,3)) = 3$ and $\text{ord}((1\,2\,3\,4)) = 4$, so $\text{ord}(\sigma) = \text{lcm}(3, 4) = 12$. Now, in order for some $\tau \in S_6$ to have order 12 we need either a 3-cycle and a 4-cycle (disjoint), or a 12-cycle, neither of which exist in S_6. □

Problem 5. (10 points)

(a) Let G be a group, and let $g \in G$. The *centralizer* of g in G is defined to be the set of elements in G that commute with g:

$$\text{C}_G(g) = \{h \in G \mid gh = hg\}.$$

Show that $\text{C}_G(g) \subseteq G$ is a subgroup.

Proof. Fix $x, y \in \text{C}_G(g)$. Then $(xy^{-1})g(xy^{-1})^{-1} = x(y^{-1}gy)x^{-1} = xgx^{-1} = g$, so by the subgroup criterion, $\text{C}_G(g) \subseteq G$ is indeed a subgroup. □

(b) Find $\text{C}_{S_n}((12\cdots n))$.

Proof. First note that $\langle(1\,2\cdots n)\rangle \subseteq \text{C}_{S_n}((1\,2\cdots n))$. Furthermore, any $\sigma \in \text{C}_{S_n}((1\,2\cdots n))$ must satisfy $\sigma(1\,2\cdots n)\sigma^{-1} = (1\,2\cdots n)$, so $(\sigma(1)\,\sigma(2)\cdots\sigma(n)) = (1\,2\,\ldots\,n)$, whence $\sigma \in \langle(1\,2\cdots n)\rangle$. □

13 Mon. 29/10/18 – group actions

Definition 13.1. Let G be a group, X a set; a **(left) action** of G on X is a function $\star : G \times X \to X$ satisfying

(a) $1 \star x = x$ for all $x \in X$;

(b) For all $a, b \in G$ and $x \in X$, $a \star (b \star x) = (ab) \star x$.

Examples;

- $G = D_8$, and X either the set of vertices of the square, or edges of the square, or diagonals of the square; D_8 acts naturally on any of these sets.
- With X any set and $G = S_X$, a natural action is given by $\sigma \star x = \sigma(x)$ for $\sigma \in S_X$ and $x \in X$.
- With G any group and $X = G$, we define the **left regular action** as $g \star x = gx$; the **right regular action** as $g \star x = xg^{-1}$; and the **action by conjugation** as $g \star x = gxg^{-1}$.
- With G any group and $H \subset G$ a subgroup, let $X = G/H$ and define the action $a \star gH = agH$. Note that this is well-defined even if H is not normal.

13.1 Actions and permutations

Let G be a group acting on a set X. Fix $g \in G$; this gives a function

$$\begin{aligned} \sigma_g : X &\to X \\ x &\mapsto g \star x. \end{aligned}$$

Note that for all $a, b \in G$, we have $\sigma_a \circ \sigma_b = \sigma_{ab}$ by the second property of group actions; hence for any $g \in G$, we have $\sigma_g \circ \sigma_{g^{-1}} = 1$, the identity on X. Thus σ_g is a bijection with inverse $\sigma_{g^{-1}}$, and we get a homomorphism

$$\begin{aligned} G &\to S_X \\ g &\mapsto \sigma_g. \end{aligned}$$

Proposition 13.2. *Given a group G and a set X, there is a correspondence*

$$\{\textit{actions of } G \textit{ on } X\} \iff \{\textit{homomorphisms } G \to S_X\}.$$

We have shown one direction; the other goes as follows. Given a homomorphism $f : G \to S_X$, we define a left-action by $g \star x = f(g)(x)$; note that $f(1) = 1 \in S_X$, so $1 \star x = x$, and $a \star (b \star x) = f(a)\,[f(b)(x)] = [f(a) \circ f(b)]\,(x) = f(ab)(x) = (ab) \star x$, the penultimate equality by f being a homomorphism.

Example; we have $|S_3| = 6$, and by HW#1 $S_3 \simeq D_6$. We will use the proposition to provide an alternative proof of this isomorphism, by finding an action of D_6 on a set with 3 elements.

Label the vertices of a triangle by $\{1, 2, 3\}$. Our group D_6 acts naturally on the labels, giving a homomorphism $D_6 \to S_3$. Since $|S_3| = 6 = |S_3|$, we only need to show that this

homomorphism has trivial kernel to get an isomorphism. In fact, any symmetry that fixes the three vertices has to fix the entire triangle, and thus be the identity on D_6. Hence our map $D_6 \to S_3$ is indeed an isomorphism.

Theorem 13.3 (Cayley)**.** *Let G be any group. Then G is isomorphic to a subgroup of a symmetric group S_X for some set X. In particular, we can take $|X| = |G|$, so if G is finite, it is isomorphic to a subgroup of S_n for some n.*

Proof. Consider the action of G on itself given by $g \star x = gx$. By our previous correspondence proposition, we get a homomorphism $f : G \to S_G$, whose kernel is in fact $\{1\}$, since $g \star 1 = 1$ in particular implies $g = 1$. Thus $G \simeq \text{im}(f) \subseteq S_G$. □

While interesting, Cayley's theorem will not prove useful on the long run, since permutation groups are quite complicated. What we get from it is the certainty that, at some level, all groups are glorified permutation subgroups.

13.2 More terminology

Let G be a group acting on a set X.

- The **kernel of the action** is the kernel of $G \to S_X$, i.e. the elemnts of G which act trivially on X.

  We say that an action is **faithful** if its kernel is $\{1\}$.
- Given an element $x \in X$, its **stabilizer** is

  $$\text{Stab}_G(x) = \{g \in G \mid g \star x = x\},$$

  and is in fact a subgroup of G.

14 Wed. 31/10/18 – Orbit-Stabilizer theorem

Theorem 14.1 (Orbit-Stabilizer)**.** *Let G be a finite set acting on a set X. Then, for any $x \in X$, we have*

$$|G| = |Gx| \cdot |\operatorname{Stab}_G(x)|.$$

15 Fri. 02/10/18 – conjugation

Examples;

- If G is abelian, then $[g] = \{g\}$.
- For $G = S_n$, we have $\sigma(i_1 \cdots i_m)\sigma^{-1} = (\sigma(i_1) \ldots \sigma(i_m))$, so $[\tau]$ = set of permutations of the same cycle type.
- For $G = \mathrm{GL}_2(\mathbb{C})$, two matrices g and g' are "similar" if they are conjugate, i.e. $g' = hgh^{-1}$ for some $h \in \mathrm{GL}_2(\mathbb{C})$.

  The different conjugacy classes are given by the Jordan normal form; any $g \in \mathrm{GL}_2(\mathbb{C})$ is conjugate to exactly one of

$$\begin{pmatrix} a & & 0 \\ & \ddots & \\ 0 & & a \end{pmatrix}, a \in \mathbb{C}^\times \mid \begin{pmatrix} a & & 1 \\ & \ddots & \\ 0 & & a \end{pmatrix}, a \in \mathbb{C}^\times \mid \quad \begin{pmatrix} a & & 0 \\ & \ddots & \\ 0 & & b \end{pmatrix}, a \neq b, a, b \in \mathbb{C}^\times.$$

The following example illustrates the intuition behind conjugation. Suppose I mail you a hexagon, and I want you to apply a reflection τ along a line L joining opposing sides. While the hexagon is in the mail, some arbitrary permutation σ is applied, and you receive it under this transformation. In order for you to apply exactly the same transformation, you would have to perform $\sigma\tau\sigma^{-1}$: if τ is reflection about L, then $\sigma\tau\sigma^{-1}$ is reflection about $\sigma(L)$. (more ... unclear ... ???)

There is no way for you to apply exactly τ, but you know *what conjugacy class τ is in.* (why?? ...)

Moral of the story: in a group, conjugating τ by σ means "applying σ to the description of τ".

Recall, again, that $\sigma(i_1 \cdots i_m)\sigma^{-1} = (\sigma(i_1) \cdots \sigma(i_m))$ in S_n.

For another example, consider $\mathrm{GL}_2(\mathbb{C})$ and fix $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. This matrix sends the basis vectors

$$\begin{aligned} e_1 &\mapsto ae_1 + ce_1 \\ e_2 &\mapsto be_1 + de_2. \end{aligned}$$

The conjugate hgh^{-1}, however, sends

$$\begin{aligned} he_1 &\mapsto ah(e_1) + ch(e_1) \\ he_2 &\mapsto bh(e_1) + dh(e_2). \end{aligned}$$

Another example; consider the normal subgroup $A_5 \subseteq S_5$. It consists of the identity, 3-cycles (abc), $(2,2)$-cycles $(ab)(cd)$ and 5-cycles $(abcde)$. It could happen that $\tau, \tau' \in A_5$ were conjugate in S_5 but *not* in A_5. For instance, let $\tau = (12345)$, and $\tau' = (45)(12345)(45)^{-1} = (12354)$. If $\sigma \in S_5$ satisfies $\sigma\tau\sigma^{-1} = \tau'$, let $\rho = \sigma^{-1}(45)$, so that $\rho\tau\rho^{-1} = \sigma^{-1}(45)\tau(45)^{-1}\sigma = \sigma\tau'\sigma^{-1} = \tau$, so $\rho \in \mathrm{C}_{S_5}(\tau)$. In fact, we have a bijection

$$\begin{aligned} \{\sigma \in S_5 \text{ s.t. } \sigma\tau\sigma^{-1} = \tau'\} &\Longleftrightarrow \mathrm{C}_{S_5}(\tau) \\ \sigma &\mapsto \sigma^{-1}(45). \end{aligned}$$

If $\mathrm{C}_{S_5}(\tau) \subseteq A_5$, then every $\sigma \in S_5$ that conjugates τ to τ' must *not* be in A_5. Since $\mathrm{C}_{S_5}(\tau) = \langle\tau\rangle \subseteq A_5$, we conclude that τ and τ' are not conjugate in A_5. Furthermore, by the orbit-stabilizer theorem,

$$\frac{[\tau]_{S_5}}{[\tau]_{A_5}} = \frac{[S_5 : \langle\tau\rangle]}{[A_5 : \langle\tau\rangle]} = \frac{|S_5|}{|A_5|} = 2,$$

so there are two conjugacy classes of 5-cycles in A_5, namely $[\tau]_{A_5}]$ and $[\tau']_{A_5}$. Taking this principle further:

Proposition 15.1. *All 3-cycles in A_5 are conjugate.*

Proof. We only need to show that any 3-cycle, say (abc), is conjugate to (123). Start with some $\sigma \in S_5$ with $\sigma(1) = a$, $\sigma(2) = b$, $\sigma(3) = b$ and arbitrary values for 4 and 5. If $\sigma \in A_5$, we are done. Otherwise, let $\sigma' = \sigma(45) \in A_5$: note that $\sigma'(123)(\sigma')^{-1} = (abc)$. This time $\mathrm{C}_{S_5}((123)) \not\subseteq A_5$, by $(45) \in \mathrm{C}_{S_5}((123))$. □

16 Mon. 05/11/18 – A_5 is simple and groups of order pq

16.1 A_5 is simple

Last time, we found the conjugacy classes that partition $A_5 \trianglelefteq S_5$. We had

- $[(1\,2\,3\,4\,5)]_{S_5} = [(1\,2\,3\,4\,5)]_{A_5} \coprod [(1\,2\,3\,5\,4)]_{A_5}$,
- $[(1\,2\,3)]_{S_5} = [(1\,2\,3)]_{A_5}$, and
- $[(1\,2)(3\,4)]_{S_5} = [(1\,2)(3\,4)]_{A_5}$.

Theorem 16.1. *A_5 is simple. (i.e. if $H \trianglelefteq A_5$, then either $H = \{1\}$ or $H = A_5$.)*

Conjugacy classes are useful in proving this because they impose restrictions on normal subgroups: if you contain an element of a conjugacy class, you contain the entire conjugacy class.

Proof. Suppose that $H \neq \{1\}$, and pick $\sigma \in H$ with $\sigma \neq 1$.

Case 1: σ is a 3-cycle. Then H has all 3-cycles, since they are contained in the same conjugacy class. Furthermore, we know that the 3-cycles generate A_5 (HW#?), so $H = A_5$.

Case 2: $\sigma = (a\,b)(c\,d)$, with $\{a, b, c, d, e\} = \{1, \ldots, 5\}$. Consider $\sigma' = (c\,d\,e)\sigma(c\,d\,e)^{-1} = (a\,b)(d\,e) \in H$ by normality. Hence $\sigma\sigma' = (a\,b)(c\,d)(a\,b)(d\,e) = (c\,d\,e) \in H$, so we go back to Case 1.

Case 3: $\sigma = (a\,b\,c\,d\,e)$. Let $\sigma' = (a\,b\,c)\sigma(a\,b\,c)^{-1} = (b\,c\,a\,d\,e) \in H$ again by normality. Then $\sigma^{-1}\sigma' = (a\,c\,e) \in H$, so we go back to Case 1. □

16.2 Groups of order pq, intro

(On the homework, we prove that if $|G| = p^2$, then $G \simeq \mathbb{Z}/p^2\mathbb{Z}$ or $\simeq (\mathbb{Z}/p\mathbb{Z})^2$.)

Tools we have:

Theorem 16.2. *Let G be a finite group, and let $H \subseteq G$ be a subgroup with $[G : H] = p$ prime, such that p is the smallest prime factor of $|G|$. Then $H \trianglelefteq G$.*

We already know this for $p = 2$.

For a counterexample showing that we truly need p to be the smallest divisor of $|G|$, we consider $\langle(1\,2)\rangle \subseteq S_3$, which has index 3 but is *not* normal.

Proof. Consider the left-regular action of G on G/H. It corresponds to a homomorphism $f : G \to S_p$, and notice that $a \in \ker f$ implies $a(bH) = bH$ for every coset, so in particular $aH = H$, i.e. $a \in H$ so $\ker f \subseteq H$.

By the first isomorphism theorem we have $|\operatorname{im} f| \mid |G|$, and by the properties of homomorphisms we have $|\operatorname{im} f| \mid |S_p| = p! = p\prod_q q$ where the rightmost product is over a number of primes $< p$. But this implies $|\operatorname{im} f| = p$, since p is the smallest prime dividing $|G|$, and so by the first isomorphism theorem again we get $|G/\ker f| = [G : \ker f] = p$.

Therefore $\ker f \subseteq H \subseteq G$ both have index p in G, which implies $\ker f = H$. Hence H is normal in G, since it is the kernel of a homomorphism. □

Theorem 16.3 (Cauchy)**.** *If G is a finite group and $p \mid |G|$ for some prime p, then G contains an element of order p.*

We do not need the full power of Cauchy's theorem, so we prove only the abelian case.

Proof. Induction on $|G|$. Let $a \in G$, with $a \neq 1$. Then, either

- $p \mid \operatorname{ord}(a)$, in which case $a^{\frac{\operatorname{ord}(a)}{p}}$ is an element of order p.
- $p \nmid \operatorname{ord}(a)$, in which case we consider $G/\langle a \rangle$, which forms a group by G being abelian and hence every subgroup normal. Then $|G/\langle a \rangle| \cdot |\langle a \rangle| = |G|$. We have that p divides the right-hand side, so it must divide the left-hand side: but $p \nmid \operatorname{ord}(a)$, so it must divide $|G/\langle a \rangle|$. By the inductive hypothesis, we get some coset $g\langle a \rangle \in G/\langle a \rangle$ of order p. Now consider the natural homomorphism $G \to G/\langle a \rangle$ sending elements to their cosets: we immediately get that $p \mid \operatorname{ord}(g)$, and we are back to the first case.

□

Corollary 16.4. *If G is an Abelian group of order $|G| = p_1 \cdots p_k$, for pair-wise distinct primes, then G is cyclic.*

Proof. We have an element $g_i \in G$ of order p_i for each i. Then $g = g_1 \cdots g_k$ has order $\gcd(p_1, \ldots, p_k) = |G|$, and so G is cyclic. □

17 Wed. 07/11/18 – class equation, pq, and Sylow's first theorem

17.1 Class equation

Let G be a group. Recall that $|[g_i]|| = 1$ iff $g_i \in \mathrm{Z}(G)$. We can write G in terms of its conjugate classes,

$$G = \coprod_{\substack{\text{conj. classes} \\ [g_i]}} [g_i] = (\mathrm{Z}(G)) \coprod \left(\coprod_{\substack{\text{non-central} \\ \text{conj. classes } [g_i]}} [g_i] \right),$$

which implies

$$|G| = |\,\mathrm{Z}(G)| + \sum_{[g_i]} |[g_i]| = |\,\mathrm{Z}(G)| + \sum_{[g_i]} [G : \mathrm{C}_G(g_i)].$$

Notice that, by Lagrange, each $[G : \mathrm{C}_G(g_i)]$ divides $|G|$, as well as $|\,\mathrm{Z}(G)|$, so the right-hand side is an expression of $|G|$ as a sum of some of its own divisors. This will prove useful.

For example (this is HW#?), if G is a p-group with $|G| = p^a$, then $\mathrm{Z}(G) \neq \{1\}$. For otherwise, (...).

Theorem 17.1. *Let G have order pq, both prime, with $p > q$. Then either*

- *G is cyclic; or*
- *G is non-abelian, and $p \equiv 1 \pmod{q}$.*

For example, $15 = 3 \cdot 5$, $35 = 7 \cdot 5$, $77 = 11 \cdot 7$ are all cyclic. For the non-cyclic case, we will eventually give a group of order pq unique up to isomorphism; this will completely classify groups of order pq as either cyclic, or that other group.

Proof. Notice that by Lagrange's, the only subgroups and elements of G have order 1, p, q, or pq.

It is a useful approach, in general, to quotient out a group by its center. So we ask, what is $|\,\mathrm{Z}(G)|$?

Case 1. $\mathrm{Z}(G) = G$, then G is Abelian, and by our last corollary, we conclude that G is cyclic.

Case 2. If $|\,\mathrm{Z}(G)| = p$ or $= q$, we show this is impossible. Take the quotient: we have that $|G/\,\mathrm{Z}(G)| = q$ or $= p$, so that $G/\,\mathrm{Z}(G)$ is cyclic since it has prime order. Using HW#3, we conclude that G is in fact Abelian, so $|\,\mathrm{Z}(G)| = pq = |G|$, a contradiction.

Case 3. If $\mathrm{Z}(G) = \{1\}$, we are in the non-abelian case. We claim that G contains elements of order p and q, which is given by Cauchy's. An alternative proof follows: by the class equation, if $x \in G$ has order p, then

$$\langle x \rangle \subseteq \mathrm{C}_G(x) \subsetneq G,$$

for if $\mathrm{C}_G(x) = G$, then $x \in \mathrm{Z}(G)$, a contradiction. But then the order of x and $\mathrm{C}_G(x)$ are sandwiched between p and $< pq$, so necessarily $\langle x \rangle = \mathrm{C}_G(x)$. Hence, by the orbit-stabilizer theorem, $|G| = |\mathrm{C}_G(x)| \cdot |[x]|$, whence $|[x]| = q$. By the same argument, for any $y \in G$ of order q, we have $|[y]| = p$. We write out the class equation,

$$pq = 1 + c_p \cdot q + c_q \cdot p,$$

where $c_p = \#$ conj. classes of elements of order p, and similarly for c_q. From this, we see that neither $c_p = 0$ nor $c_q = 0$, so we are done.

So choose $x, y \in G$ with orders p, q respectively. By a theorem from last class, we have that $\langle x \rangle \trianglelefteq G$, since $\langle x \rangle$ has index q, and q is the smallest prime dividing pq.

Hence $yxy^{-1} \in \langle x \rangle$, so $yxy^{-1} = x^k$ for some $k \in \mathbb{Z}$, and $y^2xy^{-2} = yx^ky^{-1} = x^{k^2}$, and so on and so forth. But y has order q, so $x = y^qxy^{-q} = x^{k^q}$, so $k^q \equiv 1 \pmod{p}$, and since $k \not\equiv 1 \pmod{p}$, for else $yxy^{-1} = x$, then $\langle x \rangle \subsetneq \mathrm{C}_G(x) \subsetneq G$, which is impossible (??). Therefore $\overline{k} \in (\mathbb{Z}/p\mathbb{Z})^\times$ has order q, and so $q \mid p - 1$, i.e. $p \equiv 1 \pmod{q}$. □

17.2 Sylow theorem (I)

If $n = p_1^{a_1} \cdots p_k^{a_k}$, by the Chinese remainder theorem we can write

$$\mathbb{Z}/n\mathbb{Z} \simeq (\mathbb{Z}/p_1^{a_1}\mathbb{Z}) \times \cdots (\mathbb{Z}/p_k^{a_k}\mathbb{Z}).$$

The goal is to factor any given group into "prime factors", if such thing exists in the first place.

Q: can we hope to factorize abstract groups into groups of prime power order? **No**, but we can get close.

Definition 17.2. Let G be a finite group, with $p \mid |G|$ prime. Write $|G| = p^qm$, with $(m, p) = 1$. A subgroup $H \subseteq G$ is called a **Sylow p-subgroup** if $|H| = p^q$.

Examples;

- If $G = \langle g \rangle$ is of order n, with $n = p^am$, we know that $\langle g^m \rangle$ has order p^a, and it is in fact the unique Sylow p-subgroup of G.
- If $G = S_3$, we know $|S_3| = 2 \cdot 3$: from this, we conclude that $\langle (123) \rangle$ is the unique Sylow 3-subgroup, and that $\langle (12) \rangle, \langle (23) \rangle, \langle (13) \rangle$ are all Sylow 2-subgroups.
- If $G = S_4$, we know $|S_4| = 2^3 \cdot 3$. In this case, we have that $\langle (123) \rangle$ is a Sylow 3-subgroup (not unique!), and $\langle (1234), (13) \rangle$ is a Sylow 2-subgroups.

Theorem 17.3 (Sylow I)**.** *If G is a finite group, with $p \mid |G|$ prime, then G contains a Sylow p-subgroup, which is not necessarily unique.*

Proof. Induction on $|G|$. We will consider two different inductive steps, and show that at least one of them applies.

Step 1: suppose that there is some $K \subsetneq G$ with $([G : K], p) = 1$, i.e. with index not divisible by p. If $|G| = p^am$, then $|K| = \frac{|G|}{[G:K]} = p^am'$, with $m' < m$, i.e. $|K| < |G|$. By the

inductive hypothesis, we have some $H \subset K$ with $|H| = p^a$, which is also a Sylow p-subgroup of all of G.

Step 2: suppose that there is some $K \trianglelefteq G$ with $|K| = p^b$, $b > 0$. Consider the canonical quotient map $f : G \to G/K$ sending $g \mapsto gK$. By the First Isomorphism theorem, we have $|G/K| = \frac{|G|}{|K|} = p^{a-b}m < |G|$, so by the inductive hypothesis we have a subgroup $\overline{H} \subseteq G/K$ with $|\overline{H}| = p^{a-b}$. Consider the set $H = f^{-1}(\overline{H}) \subseteq G$, which is in fact a subgroup. We have that $f(H) = \overline{H}$, and so by the First Isomorphism theorem again, we get $H/K \simeq \overline{H}$. Therefore $|H| = |\overline{H}| \cdot |K| = p^{a-b}p^b = p^a$, i.e. H is a Sylow p-subgroup of G.

Now we show that one of A or B hold. As usual, we consider the center of G.

Case 1: $p \mid |\operatorname{Z}(G)|$. Since $\operatorname{Z}(G)$ is Abelian, there is some $x \in \operatorname{Z}(G)$ of order p (by Cauchy's). Let $K = \langle x \rangle$, so that $|K| = p$ and $K \trianglelefteq G$; we can then use Step 2.

Case 2: $p \nmid |\operatorname{Z}(G)|$. Consider the class equation:

$$|G| = |\operatorname{Z}(G)| + \sum_i [G : \operatorname{C}_G(g_i)].$$

Since $p \mid |G|$ and $p \nmid |\operatorname{Z}(G)|$, there must be some i for which $p \nmid [G : \operatorname{C}_G(g_i)]$. Hence, with $K = \operatorname{C}_G(g_i)$, we can apply Step 1. $\square$

18 Fri. 9/11/18 – towards Sylow's second and third theorems

We discover the implications of Sylow's first theorem. In general, given a group G and letting $X = \{H \subseteq G \text{ subgroup }\}$, we consider the action of G on X by conjugation, i.e. $g \star H = gHg^{-1}$.

Note that $\mathrm{Stab}_G(H) = \mathrm{N}_G(H)$, and we have $H \trianglelefteq \mathrm{N}_G(H)$. The following is a very useful, though technical, lemma.

Lemma 18.1. *Let G be a finite group, p a prime dividing $|G|$. Given a Sylow p-subgroup $H \subseteq G$, and $K \subset G$ any p-subgroup, we have*

$$\mathrm{N}_G(H) \cap K = H \cap K.$$

(*Proof...*)
From this lemma follows

Corollary 18.2. *With G, H, K as in the lemma, let $\mathcal{O} = \{kHk^{-1} \mid k \in K\}$ be the orbit of H under the action of conjugation by elements in $K \subset G$. Then either*

- *$|\mathcal{O}| = 1$ and $K \subseteq H$; or*
- *$p \mid |\mathcal{O}|$ and $K \not\subseteq H$.*

It is worth pointing out a few things: first, note that $p \mid |\mathcal{O}|$ is really equivalent to saying that $|\mathcal{O}| \neq 1$, since by the orbit stabilizer $|G| = |\mathcal{O}||\mathrm{N}_G(H)|$ …(some argument) …so $p \mid |\mathcal{O}|$.

The notable part of this lemma is the *and* in the first possibility: if $K \subseteq H$, it is clear that the orbit of H under conjugation by K is just H itself. It is however not at all obvious that $|\mathcal{O}| = 1$ implies $K \subseteq H$.

Proof. We know that $K \subseteq H$ iff $H \cap K = K$, which by the technical lemma happens iff $\mathrm{N}_G(H) \cap K = K$, iff $\mathrm{Stab}_K(H) = K$, iff $|\mathcal{O}| = 1$ by the Orbit-Stabilizer theorem. □

We are ready to tackle the next big theorem.

Theorem 18.3 (Sylow II and III)**.** *Let G be a finite group, $p \mid |G|$ a prime number, and write $|G| = p^a m$ with $(p, m) = 1$.*

- *(2nd) If $H \subseteq G$ is a Sylow p-subgroup and $K \subseteq G$ is a p-subgroup, then $K \subset gHg^{-1}$ for some $g \in G$.*
- *(3rd) If n_p is the number of Sylow p-subgroups in G, then $n_p \equiv 1 \pmod{p}$ and $n_p \mid m$.*

For the 2nd theorem, by choosing K to be another Sylow p-subgroup we conclude that $K = gHg^{-1}$, so Sylow p-subgroups are in some sense "unique" up to conjugation.

For the 3rd theorem, note that the two conditions on n_p imposes a great deal of restrictions on the number of Sylow p-subgroups in a given group. We will use this to our advantage to show that in some situations, we necessarily have $n_p = 1$, which is noteworthy by the following corollary:

Corollary 18.4. *$n_p = 1$ if and only if G has a normal Sylow p-subgroup.*

Proof. ($\Longrightarrow$) Given a Sylow p-subgroup $H \subseteq G$, for all $g \in G$ we have that gHg^{-1} is a Sylow p-subgroup by the second Sylow theorem, but since H is the only Sylow p-subgroup of G, we necessarily have $gHg^{-1} = H$, so H is normal in G.

($\Longleftarrow$) Let $H \trianglelefteq G$ be a normal Sylow p-subgroup. For any other Sylow p-subgroup $K \subseteq G$, by the second Sylow theorem we have that $K = gHg^{-1}$ for some $g \in G$, but H is normal in G so $gHg^{-1} = H$, i.e. $K = H$. $\square$

19 Mon. 12/11/18 – proof of Sylow's, applications

19.1 Sylow theorem (II) and (III)

We now prove the 2nd and 3rd of Sylow's theorems.

Proof of 2nd theorem. Let $X = \{gHg^{-1} \mid g \in G\}$ be the orbit of H under conjugation by elements in G. We let G act on X by conjugation, i.e. $h \star gHg^{-1} = hgHg^{-1}h^{-1}$. We note that any subgroup of G also acts by this action.

The reasonable thing to do would be to consider the action for $K \subseteq G$ in particular, because we want to show that $K \subset gHg^{-1}$. Instead, we consider the action of H itself. We write the decomposition of X into orbits:

$$X = \{H\} \coprod \mathcal{O}_1 \coprod \cdots \coprod \mathcal{O}_r.$$

Fix some $g_iHg_i^{-1} \in \mathcal{O}_i$, so $H \neq g_iHg_i^{-1}$ and thus $H \subsetneq g_iHg_i^{-1}$. We use the technical corollary to get that $p \mid |\mathcal{O}_i|$, so $X \equiv 1 \pmod{p}$.

We now consider the action of K on X, and write again

$$X = \mathcal{O}'_1 \coprod \cdots \coprod \mathcal{O}'_s,$$

but $p \nmid |X|$, so there must be some orbit for which $p \nmid |\mathcal{O}'_i|$, so necessarily $|\mathcal{O}'_i| = 1$, and by the corollary again (using the magical direction this time), we get $K \subset gHg^{-1}$. □

Proof of 3rd theorem. Let X be the set of all Sylow p-subgroups, so $n_p = |X| \equiv 1 \pmod{p}$ by an intermediate step in our previous proof.

Furthermore, by the Orbit-Stabilizer theorem, we have $|G| = |X||\mathrm{N}_G(H)|$ so $|X| = [G : \mathrm{N}_G(H)]$. But since $H \subseteq \mathrm{N}_G(H)$, we have $[G : \mathrm{N}_G(H)] \mid [G : H] = m$.

We conclude that $n_p \equiv 1 \pmod{p}$ and $n_p \mid m$. □

We now have an easy re-proof of Cauchy's. Suppose that $p \mid |G|$ is prime. By the first Sylow theorem, we know that G has a Sylow p-subgroup $H \subseteq G$. Choose any $x \in H$ with $x \neq 1$. Then by Lagrange's we necessarily have $\mathrm{ord}(x) = p^b$ with $b > 0$, so take $x^{p^{b-1}}$, which has order p.

Corollary 19.1. *Let G be a finite group, with $p \mid |G|$ prime. Then for any $x \in G$, its order is p^b if and only if $x \in H$ for some Sylow p-subgroup $H \subseteq G$.*

In particular, if G has a normal Sylow p-subgroup H, then H consists uniquely of elements in G whose order are powers of p.

Proof. ($\Longleftarrow$) Just proved it by Lagrange's.

($\Longrightarrow$) Consider the subgroup $\langle x \rangle$, which is in particular a p-subgroup of G. By the second Sylow theorem, $\langle x \rangle$ is contained in some Sylow p-subgroup of G, and thus x is as well. □

Corollary 19.2. *If G has a normal Sylow p-subgroup and $a, b \in G$ have order p^x and p^y respectively, then ab has order p^z for some integer z.*

Proof. Let H be the unique normal Sylow p-subgroup of G. By the previous corollary, both a and b are in H. By closure under multiplication we have $ab \in H$, but again by the corollary ab must have order a power of p. □

20 Wed. 14/11/18 – examples and the Structure Theorem

20.1 Groups of order 1225

We have seen how the case when $n_p = 1$ is extremely useful in order to know more about a given group. For example, suppose that $|G| = 1225 = 5^2 7^2$.

From the fact that $n_5 \mid 49$, we have that $n_5 = 1, 7, 49$, but since $n_5 \equiv 1 \pmod 5$, we reduce the possibilities to $n_5 \equiv 1, 2, 4 \pmod 5$ and thus conclude that $n_5 = 1$.

Similarly for $n_7 \mid 25$, so we have $n_7 = 1, 5, 25$, but by $n_7 \equiv 1, 5, 4 \pmod 7$ we conclude again that $n_7 = 1$.

Hence G has normal subgroups H_5 and H_7 of order $|H_5| = 25$ and $|H_7| = 49$. What can we learn about G from this? Turns out that quite a bit.

Lemma 20.1. *Let G be a group, and suppose that it has normal subgroups $H, K \trianglelefteq G$ such that $H \cap K = \{1\}$. Then $hk = kh$ for all $h \in H$ and $k \in K$.*

Proof. We know that $hk = kh$ iff $hkh^{-1}k^{-1} = 1$. We call this element the **commutator** of h and k.

Fix any two elements $h \in H$, $k \in K$. Parenthesizing, we note that $(hkh^{-1})k^{-1}$ is in K and that $h(kh^{-1}k^{-1})$ is in H, so $hkh^{-1}k^{-1} \in H \cap K = \{1\}$, and thus by our observation we conclude that h and k commute. □

Theorem 20.2. *Let G be a group and $H, K \trianglelefteq G$ normal subgroups with $H \cap K = \{1\}$. Then the map*

$$\begin{aligned} f : H \times K &\to HK \\ (h, k) &\mapsto hk \end{aligned}$$

is an isomorphism.

We call HK the **internal product** and $H \times K$ the **external product** of subgroups H and K.

This relates to the linear algebra facts that, given two disjoint subspaces $V_1, V_2 \subseteq V$ of a vector space, we have $V_1 \oplus V_2 \simeq V_1 + V_2$.

Proof. Showing that the map f is a homomorphism requires using the lemma we have just proven.

For surjectivity, it is clear that any product $hk \in HK$ is mapped to by the pair $(h, k) \in H \times K$.

If $f((h, k)) = 1$, then $hk = 1$ so $h = k^{-1}$, but then $k \in H$ so $k = 1$ and thus $h = 1$. Hence f is also injective, and thus an isomorphism. □

We now apply this result to our $|G| = 1225$ case. Note that $(|H_5|, |H_7|) = 1$, so these subgroups have trivial intersection, and so we apply the theorem to get that $H_5 \times H_7 \simeq H_5 H_7 \subseteq G$. However, note that $|H_5 \times H_7| = |G|$, and so $G = H_5 H_7 \simeq H_5 \times H_7$.

Furthermore, by Homework #5 we know that $|H| = p^2$ implies that H is either isomorphic to $\mathbb{Z}/p^2\mathbb{Z}$ or $(\mathbb{Z}/p\mathbb{Z})^2$. Hence, up to isomorphism, G is reduced to one of four possibilities, which is amazing considering that all we knew about G was its order!

This lends itself to a general result:

Theorem 20.3. *Let G be a finite group with $|G| = p_1^{a_1} \cdots p_k^{a_k}$. Suppose that for each i, we have a normal Sylow p-subgroup $H_{p_i} \trianglelefteq G$, i.e $n_{p_i} = 1$. Then*

$$G \simeq H_{p_1} \times \cdots \times H_{p_k}.$$

The assumptions of the things we got lucky for $|G| = 1225$: we ruled out any possibilities other than $n_5 = n_7 = 1$. Furthermore (this is not captured in the theorem), each H_p was of order prime squared, which made things even easier. The proof is not magical, we use induction and the previous result.

Proof. We note that if $H, K \trianglelefteq G$ are normal, then HK is also normal.

So $H_{p_1} \dots H_{p_i}$ and $H_{p_{i+1}}$ are normal in G, with trivial intersection by their orders being relatively prime. We apply the previous theorem to get

$$(H_{p_1} \cdots H_{p_i}) \times H_{p_{i+1}} \simeq H_{p_1} \cdots H_{p_i} H_{p_{i+1}}.$$

Hence we have shown that

$$H_{p_1} \times \cdots \times H_{p_k} \simeq H_{p_1} \cdots H_{p_k} \subseteq G,$$

but the order of the right-hand side of the equation is equal to the order of G (by the isomorphism to the external product), and thus must be equal to G. □

Hic sunt dracones! Having normal subgroups $H_1, H_2, H_3 \trianglelefteq G$ with pair-wise trivial intersection does *not* imply $H_1 \times H_2 \times H_3 \simeq H_1H_2H_3$, because the intersection $H_1H_2 \cap H_3$ might not necessarily be trivial anymore. We truly needed the assumption on H_i being Sylow p-subgroups.

20.2 Structure Theorem

If G is abelian, then $n_p = 1$ for all primes dividing $|G|$ because every subgroup is normal, so our previous theorem always applies to abelian groups. With some more algebra, we get this result.

Theorem 20.4 (Structure theorem for finite abelian groups)**.** *If G is an abelian p-group, then $G \simeq \mathbb{Z}/p^{a_1}\mathbb{Z} \times \cdots \mathbb{Z}/p^{a_l}\mathbb{Z}$ for unique exponents up to reordering.*

If G is a finite abelian group, then $G \simeq H_{p_1} \times \cdots \times H_{p_k}$ with H_{p_i} abelian p_i-groups unique up to isomorphism.

21 Fri. 16/11/18 – Midterm II

Problem 1. (10 points) True or false. Write one or two sentences justifying your answer:

(a) If a group G acts on a finite set X, then the size of any orbit divides $|X|$.

Answer. False. By the Orbit-Stabilizer theorem, we have that the size of any orbit divides $|G|$, not $|X|$. For a counterexample, consider the usual action of $\langle(1\,2)\rangle \subseteq S_3$ on $X = \{1, 2, 3\}$, which has an orbit $\{1, 2\}$ the order of which does not divide $|\langle(1\,2)\rangle| = 3$. □

(b) If G is a simple group of order p^n for some prime p, then $G \simeq \mathbb{Z}/p\mathbb{Z}$.

Answer. True. Since G is a p-group, we have some $x \in \mathrm{Z}(G)$ with $\mathrm{ord}(x) = p$. Hence $\langle x\rangle$ is normal, so necessarily $G = \langle x\rangle \simeq \mathbb{Z}/p\mathbb{Z}$. □

(c) $\mathrm{C}_{S_8}((1\,2)(3\,4)(5\,6))$ contains an element of order 3.

Answer. True. For example, $(1\,3\,5)(2\,4\,6)$. As an alternative, notice that $|\mathrm{C}_{S_8}((1\,2)(3\,4)(5\,6))| = (3!2^3)2!$ (by some HW#? formula), so by Cauchy's this group has an element of order 3. □

(d) If G is a finite group such that there is a prime $p^2 \mid |G|$, and H a subgroup of index p, then G is not simple.

Answer. False, but tricky. By the orbit-stabilizer, it is not necessarily true that $m \mid |G|$ is G acts faithfully on a set with m elements, so it is reasonable to suspect that this is false.

For an explicit counterexample, consider $G = \mathbb{Z}/n\mathbb{Z}$, and the question becomes *"if m is the smallest integer such that a"*. □

(e) If H and K are finite subgroups of G, then $[K : H \cap K] \mid [G : H]$.

Answer. False. For example, $H = \langle(1\,2)\rangle$, $K = \langle(2\,3)\rangle$ in $G = S_3$. We have $[G : H] = 3$ and $[K : H \cap K] = 2$. □

Problem 2. (5 points) Let $n \geq 2$ be an integer. The group S_n acts on the set

$$X = \{1, \ldots, n\} \times \{1, \ldots, n\}$$

via $\sigma \star (i, j) = (\sigma(i), \sigma(j))$. Find the orbits for this action, and for each orbit find the size of the orbit as well as the size of the stabilizer of an element in that orbit.

Proof. □

Problem 3. (5 points) Show that $(\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z})/\langle(2, \overline{2})\rangle \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Proof. □

Problem 4. (5 points) Let G be a group and let $H \subseteq G$ be a normal subgroup such that the quotient group G/H is abelian. Show that $[g] \subseteq gH$ for any $g \in G$, where $[g]$ denotes the conjugacy class of g in G.

Proof. We have $kgk^{-1}H = (kH)(gH)(k^{-1}H) = (kH)(k^{-1}H)(gH) = gH$, so $kgk \in gH$. □

Problem 5. (5 points) Let G be a finite group and suppose that there is a prime p for which $p^2 \mid |G|$, and G contains a subgroup H of index p. Show that G is not simple.

Proof. Consider the action of G on G/H. This gives a homomorphism $\varphi : G \to S_p$. We want to show that the kernel of this action is *not* trivial. Since $\operatorname{im}(f) \mid p!$, then $p^2 \nmid \operatorname{im}(f)$ so we must have $p \mid |\ker \varphi|$, giving a nontrivial kernel which is in fact contained in H. This proves the statement. □

Problem 6. (5 points) Suppose that G is finite, and that any two non-identity elements in G are conjugate. Show that $G \simeq \mathbb{Z}/2\mathbb{Z}$.

Proof. The orbit of any non-identity element has cardinality $|G| - 1$. Hence, by the Orbit-Stabilizer theorem, we have $|G| = (|G| - 1)|\operatorname{Stab}_G(x)|$.

This immediately implies that $|G| = 2$, so $G \simeq \mathbb{Z}/2\mathbb{Z}$. □

22 Mon. 19/11/18 – The semidirect product

22.1 Motivation

Recall our theorem from the previous class, the backbone of our proof for understanding $|G| = 1225$.

Let G be a group, $H, K \trianglelefteq G$ with $H \cap K = \{1\}$. Then $H \times K \simeq HK$ through $(h, k) \mapsto hk$.

The question is: can we relax the requirement that *both* H and K be normal? The answer is **yes**, and we show this by the semidirect product.

Recall that $HK \subseteq G$ is indeed a subgroup; this is also true even if only H is normal in G, for

$$hk \cdot h'k' = h(kh'k^{-1})kk' \in HK$$

and

$$(hk)^{-1} = k^{-1}h^{-1} = (k^{-1}h^{-1}k)k^{-1} \in HK.$$

We want to encode the action of K on H by conjugation. Fixing $k \in K$, we have an automorphism

$$\begin{aligned} \varphi(k) : H &\to H \\ h &\mapsto khk^{-1}. \end{aligned}$$

We quickly check that this is in fact an automorphism:

$$\begin{aligned} \varphi(k)(hh') &= khh'k^{-1} = khk^{-1}kh'k^{-1} \\ &= \varphi(k)(h)\varphi(k)(h'), \end{aligned}$$

and $\varphi(k^{-1})$ is an inverse to $\varphi(k)$.

Going one level up, we have a homomorphism

$$\begin{aligned} \varphi : K &\to \mathrm{Aut}(H) \\ k &\mapsto \varphi(k). \end{aligned}$$

Indeed, we have

$$\begin{aligned} \varphi(kk')(h) &= (kk')h(kk')^{-1} = k(k'hk'^{-1})k^{-1} \\ &= k\varphi(k')(h)k^{-1} = \varphi(k)\left(\varphi(k')(h)\right) \\ &= (\varphi(k) \circ \varphi(k'))(h). \end{aligned}$$

In a very concrete sense, as we will see, this homomorphism encodes all the information about the action of K on H, which in turn characterizes the product HK.

22.2 Formal definition

Definition 22.1. Given groups H and K, together with a homomorphism $\varphi : K \to \mathrm{Aut}(H)$, we define the **semidirect product** $H \rtimes_\varphi K$ in two steps:

- as a set, $H \rtimes_\varphi K$ is simply $H \times K$;
- the binary operation on $H \rtimes_\varphi K$ is given by

$$(h, k)(h', k') = (h\varphi(k)(h'), kk').$$

Proposition 22.2. *$H \rtimes_\varphi K$ is a group.*

Proof. The identity is $(1, 1)$, for

$$\begin{aligned}(1, 1)(h, k) &= (1\varphi(1)(h), 1k) = (h, k) \quad \text{and} \\ (h, k)(1, 1) &= (h\varphi(k)(1), k1) = (h, k).\end{aligned}$$

As for closure of multiplication, we have

$$(h, k)(h', k') = (h\varphi(k)(h'), kk') \in H \rtimes_\varphi K.$$

The inverse of an element (h, k) is $(\varphi(k^{-1})(h^{-1}), k^{-1})$, for

$$\begin{aligned}(h, k)(\varphi(k^{-1})(h^{-1}), k^{-1}) &= \left(h\varphi(k)\left(\varphi(k^{-1})(h^{-1})\right), kk^{-1}\right) \\ &= (h\varphi(kk^{-1})(h^{-1}), 1) = (h\varphi(1)(h^{-1}), 1) = (hh^{-1}, 1) = (1, 1) \quad \text{and} \\ (\varphi(k^{-1})(h^{-1}), k^{-1})(h, k) &= (\varphi(k^{-1})(h^{-1})\varphi(k^{-1})(h), k^{-1}k) \\ &= (\varphi(k^{-1})(h^{-1}h), 1) = (\varphi(k^{-1})(1), 1) = (1, 1).\end{aligned}$$

Finally, we check that associativity holds.

> Common sense says that you shouldn't check associativity on the board, but I don't like common sense.
>
> George Boxer

$$((h, k)(h', k'))\,(h'', k'') = \cdots$$

□

Here's the punchline: we show that both H and K are embedded in $H \rtimes_\varphi K$, and we generalize the theorem we posed at the start of the class.

Proposition 22.3. *$\{(h, 1) \mid h \in H\}$ is a subgroup of $H \rtimes_\varphi K$ isomorphic to H.*

Proof. The isomorphic part is clear. As for being a subgroup,

$$(h, 1)(h', 1) = (h\varphi(1)(h'), 1) = (hh', 1).$$

□

Proposition 22.4. *$\{(1,k) \mid k \in K\}$ is a subgroup of $H \rtimes_\varphi K$ isomorphic to K.*

Proof. Indeed,

$$(1,k)(1,k') = (1\varphi(k)(1), kk') = (1, kk').$$

□

Furthermore, we have a very nice conjugation formula for K on H:

$$\begin{aligned}(1,k)(h,1)(1,k)^{-1} &= (1,k)(h,1)(1,k^{-1}) \\ &= (1\varphi(k)(h), k)(1,k^{-1}) \\ &= (\varphi(k)(h)\varphi(k)(1), kk^{-1}) \\ &= (\varphi(k)(h), 1),\end{aligned}$$

which somehow generalizes usual conjugation of K on H in our initial example.

Theorem 22.5. *Given a group G, subgroups $H, K \subseteq G$ with $H \trianglelefteq G$ and $H \cap K = \{1\}$, and a homomorphism $\varphi : K \to \mathrm{Aut}(H)$ given by $\varphi(k)(h) = khk^{-1}$, then the map*

$$\begin{aligned}f : H \rtimes_\varphi K &\to HK \\ (h,k) &\mapsto hk\end{aligned}$$

is an isomorphism.

Proof. We first check that it is a homomorphism:

$$\begin{aligned}f((h,k))f((h',k')) &= hkh'k' \\ &= hkh'k^{-1}kk' \\ &= h\varphi(k)(h')kk' \\ &= f((h\varphi(k)(h'), kk')) \\ &= f((h,k)(h',k')).\end{aligned}$$

It is clear that surjectivity holds, since for any $hk \in HK$ we have $f((h,k)) = hk$.

Finally, suppose that $f((h,k)) = 1$, then $hk = 1$ so $h = k^{-1} \in H \cap K = \{1\}$, so $h = k = 1$. Hence the map is injective. □

23 Wed. 21/11/18 – Examples of the semidirect product

Recall that we form the semidirect product from two given groups H and K, by taking a homomorphism $\phi : K \to \mathrm{Aut}(H)$. The resulting semidirect product $H \rtimes_\phi K$ is set-isomorphic to $H \times K$, but its group law is given by

$$(h, k)(h', k') = (h\phi(k)(h'), kk').$$

We proved that $H \rtimes_\phi K$ is indeed a group. If H and K are taken to be subgroups of some larger G, with H normal and $H \cap K = \{1\}$, then the resulting semidirect product $H \rtimes_\phi K$ is isomorphic to HK through the obvious map, with ϕ denoting conjugation in H by K.

23.1 Dihedral group D_{2n}

Let H be the subgroup of rotations in D_{2n}, which is normal and isomorphic to $\mathbb{Z}/n\mathbb{Z}$. Let K be the subgroup generated by a single reflection in D_{2n}, which is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. It is clear that $H \cap K = \{1\}$, so we apply the theorem to get $(\mathbb{Z}/n\mathbb{Z}) \rtimes_\phi (\mathbb{Z}/2\mathbb{Z}) \simeq H \rtimes_\phi K \simeq HK$, but since $|HK| = 2n$, we get $(\mathbb{Z}/n\mathbb{Z}) \rtimes_\phi (\mathbb{Z}/2\mathbb{Z}) \simeq D_{2n}$, with

$$\begin{aligned}\phi(1)(r^k) &= r^k \\ \phi(s)(r^k) &= sr^k s^{-1} = r^{-k}.\end{aligned}$$

With this in mind, we can now work with D_{2n} in terms of $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$: we write $D_{2n} = \{r^a s^b \mid 0 \le a < n, 0 \le b \le 1\}$, and

$$\begin{aligned}(r^a s^b)(r^{a'} s^{b'}) &= r^a (s^b r^{a'} s^{-b}) s^b s^{b'} \\ &= r^a r^{(-1)^b a'} s^{b+b'} \\ &= r^{a+(-1)^b a'} s^{b+b'}.\end{aligned}$$

23.2 Alternating group A_4

Let $G = A_4$, and let $H = \{1, (12)(34), (13)(24), (14)(23)\} \subseteq A_4$ be the Klein 4-group, which is normal and isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$. Also let $K = \langle (123) \rangle \simeq \mathbb{Z}/3\mathbb{Z}$.

Since $\gcd(|H|, |K|) = 1$, we have $H \cap K = \{1\}$ by Lagrange's, whence $A_4 \simeq (\mathbb{Z}/2\mathbb{Z})^2 \rtimes_\phi (\mathbb{Z}/3\mathbb{Z})$, with ϕ usual conjugation, which we will not spend time writing it out explicitly.

23.3 Automorphism group examples

Understanding semidirect products requires understanding automorphism groups in general, and homomorphisms of the form $K \to \mathrm{Aut}(H)$.

Example; we know from HW that $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$, because if ϕ is an automorphism of $\mathbb{Z}/n\mathbb{Z}$, it is fully determined by $\phi(1) = a$, whence $\phi(x) = ax$. In order for this map to be a bijection, we need a to be invertible.

Example; we have also seen that $\mathrm{Aut}((\mathbb{Z}/n\mathbb{Z})^2) \simeq \mathrm{GL}_2(\mathbb{F}_p)$. It follows from a similar argument: an automorphism of $(\mathbb{Z}/n\mathbb{Z})^2$ is fully determined by $\phi(1,0) = (a,c)$ and $\phi(0,1) = (b,d)$, whence $\phi(x,y) = \phi(x(1,0) + y(0,1)) = x\phi(1,0) + y\phi(0,1) = (ax+by, cx+dy)$, corresponding exactly to multiplication of the vector (x,y) by the matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

This map is invertible iff A is invertible, i.e. $\det(A) \neq 0$, iff $A \in \mathrm{GL}_2(\mathbb{F}_p)$.

23.4 Homomorphism examples

If $K = \langle y \rangle$ is cyclic of order n, then

$$\{\text{homomorphism} \quad \phi : K \to \mathrm{Aut}(H)\} \iff \{\psi \in \mathrm{Aut}(H) \mid \psi^n = 1\}.$$

So $H \rtimes_\phi \langle y \rangle = \{(h, y^a) \mid h \in H, 0 \leq a < n\}$ with group law

$$\begin{aligned}(h, y^a)(h', y^b) &= (h\phi(y^a)(h'), y^{a+b}) \\ &= (h\psi^a(h'), y^{a+b}),\end{aligned}$$

whence

$$\begin{aligned}(1, y)(h, 1) &= (\psi(h), y) \\ &= (\psi(h), 1)(1, y),\end{aligned}$$

i.e. $(1,y)(h,1)(1,y)^{-1} = (\psi(h), 1)$.

For a very concrete example, let p, q be primes with $p > q$. If G is non-abelian with $|G| = pq$, we know that $p \equiv 1 \pmod{q}$. Consider $G = (\mathbb{Z}/p\mathbb{Z}) \rtimes (\mathbb{Z}/q\mathbb{Z}) \simeq \langle x \rangle \rtimes \langle y \rangle$. We need $\psi \in \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ to have order q. Since $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}) = (\mathbb{Z}/p\mathbb{Z})^\times$, we want $k \in (\mathbb{Z}/p\mathbb{Z})^\times$ for which $k^q \equiv 1 \pmod{q}$, and $k \not\equiv 1$.

Hence we denote every such automorphism by $\psi_k(x) = x^k$, so $\psi_k(x^a) = x^{ka}$. Then

$$\langle x \rangle \rtimes_{\psi_k} \langle y \rangle = \{x^a y^b \mid 0 \leq a < p, 0 \leq b < q\},$$

with group law given by

$$(x^a, y^b)(x^{a'}, y^{b'}) = (x^{a + k^b a'}, y^{b+b'}).$$

24 Fri. 23/11/18 – no class, thanksgiving

—

25 Mon. 26/11/18 – ??

26 Wed. 28/11/18 – when Sylow's is not enough

26.1 Groups of order 30

We now explore arbitrary groups of a given order, for which Sylow's theorem does not immediately give the normal subgroup structure.

Example; let G be a group of order $30 = 2 \cdot 3 \cdot 5$. Sylow analysis gives

$$\begin{aligned} n_5 &= 1, 6 \\ n_3 &= 1, 10 \\ n_2 &= 1, 3, 5, 15. \end{aligned}$$

It turns out that $n_3 = n_5 = 1$, but it is not immediately obvious.

Claim: either $n_3 = 1$ or $n_5 = 1$.

Proof. If $n_5 = 6$, there are $6 \cdot (5-1) = 24$ elements of order 5 in G.

If $n_3 = 10$, there are $10 \cdot (3-1) = 20$ elements of order 3 in G.

These two cannot be true at the same time, since $24 + 20 > 30 = |G|$. □

Now let H_3, H_5 be Sylow 3− and 5−subgroups of G. At least one of them is normal, so

$$N = H_3 H_5 \subseteq G$$

is a subgroup of G, which has order $3 \cdot 5 = 15$, whence $[G : N] = 2$, so N is in fact normal. Therefore $N \simeq \mathbb{Z}/15\mathbb{Z}$, by our classification of groups of order pq, given that $5 \not\equiv 1 \pmod 3$.

Thus $G \simeq \mathbb{Z}/15\mathbb{Z} \rtimes_\phi \mathbb{Z}/2\mathbb{Z}$ (?? why ??).

Claim; both H_3 and H_5 are normal in G.

If $g \in G$, then $gH_3g^{-1} \subseteq gNg^{-1} = N$, by N being normal. But $N \simeq \mathbb{Z}/15\mathbb{Z}$ has a unique subgroup of order 3, so in fact we have $gH_3g^{-1} = H_3$, whence H_3 is normal. The same argument works for H_5.

This proves our initial claim. In fact, we have in general that if $|G| = 2m$ with m odd, then there is some $N \subseteq G$ such that $[G : N] = 2$ (see midterm 2 review and HW#8).

26.2 Automorphisms and characteristic subgroups

Let G be a group. For all $g \in G$, we have $\phi_g \in \mathrm{Aut}(G)$ given by $\phi_g(h) = ghg^{-1}$, and a homomorphism

$$\begin{aligned} f : G &\to \mathrm{Aut}(G) \\ g &\mapsto \phi_g, \end{aligned}$$

whose kernel is $\mathrm{Z}(G)$. Hence, by the first isomorphism theorem, we have $G/\mathrm{Z}(G) \simeq \mathrm{im}\, f$.

Definition 26.1. We say that an automorphism of the form ϕ_g is **inner**. Otherwise, we call it **outer**.

We denote by $\mathrm{Inn}(G) \subseteq \mathrm{Aut}(G)$ the subgroup of inner automorphism. In fact, we have $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$, as we shall see in HW#9. Let $\mathrm{Out}(G) = \mathrm{Aut}(G) \setminus \mathrm{Inn}(G)$.

Example; if G is abelian, then $\mathrm{Inn}(G) = \{1\}$, so $\mathrm{Out}(G) = \mathrm{Aut}(G)$.

If $G = S_n$ for $n \neq 6$, then $\mathrm{Aut}(G) = \mathrm{Inn}(G) \simeq S_n$, so $\mathrm{Out}(G) = \{1\}$.

When $n = 6$, we have $[\mathrm{Aut}(S_6) : \mathrm{Inn}(S_6)] = 2$, whence $\mathrm{Out}(S_6) \simeq \mathbb{Z}/2\mathbb{Z}$, as we shall see in the final review sheet.

Definition 26.2. A subgroup $H \subseteq G$ is called **characteristic** if $\phi(H) = H$ for all $\phi \in \mathrm{Aut}(G)$.

In particular, $\phi_g(H) = gHg^{-1} = H$, so H being characteristic implies that it is normal.

Why do we care about characteristic subgroups? Recall that having subgroups $K \trianglelefteq H \trianglelefteq G$ does not imply that K be normal in G, but

Proposition 26.3. *Suppose that $K \subseteq H \subseteq G$ are subgroups, and that K is characteristic in H. Then*

(1) $H \trianglelefteq G$ implies $K \trianglelefteq G$; and

(2) $H \subseteq G$ characteristic implies $K \subseteq G$ characteristic.

Proof of (1). For any $g \in G$ we have $gHg^{-1} = H$, so ϕ_g restricts to an automorphism of H, not necessarily inner. Then $\phi_g(K) = K$ by K being characteristic in K, so $gKg^{-1} = K$, i.e. K is normal in G. □

Example; $\langle(1,0)\rangle \subseteq (\mathbb{Z}/p\mathbb{Z})^2$. For $A \in \mathrm{GL}_2(\mathbb{F}_p)$, which is equivalent to an automorphism of $(\mathbb{Z}/p\mathbb{Z})^2$, we have $A\langle(1,0)\rangle = \langle A(1,0)\rangle$, which is not usually equal to $\langle(1,0)\rangle$, for example

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \langle \begin{pmatrix} 1 \\ 0 \end{pmatrix} \rangle = \langle \begin{pmatrix} 0 \\ 1 \end{pmatrix} \rangle.$$

If we let H be the unique subgroup of G of a given order $|H|$, then $H \subseteq G$ is characteristic. From this we get

- A normal Sylow subgroup is characteristic; and
- Any subgroup of a cyclic group is characteristic.

26.3 Our "normal subgroup" program

Problem; how do we show that a group G of some order n has a normal subgroup when we can't necessarily find a normal Sylow subgroup? Or, equivalently, how can we show that there are no simple groups of a given order n?

We explore are number of strategies; to begin with, if G is simple and we have a homomorphism $f : G \to H$, then either $\ker f = \{1\}$ or $\ker f = G$. If we furthermore assume the homomorphism to be non-trivial, we must have $\ker f = \{1\}$, so by the 1st ISO theorem we get $G \simeq \mathrm{im}\, f \subseteq H$.

In general, if we find an action of G on a set of n elements, we get a special non-trivial homomorphism

$$f : G \to S_n,$$

so if $\ker f \neq \{1\}$, we have $|G| \mid n!$. We can improve this divisibility condition a bit, by considering the sequence

$$G \to S_n \to S_n/A_n = \mathbb{Z}/2\mathbb{Z}.$$

If G is not isomorphic to $\mathbb{Z}/2\mathbb{Z}$, then necessarily $\operatorname{im} f \subseteq A_n$ implies $|G| \mid \frac{n!}{2}$, a slight improvement.

Example; there are no simple subgroups of order $72 = 2^3 \cdot 3^2$.

Sylow analysis gives $n_3 = 1, 4$ and $n_2 = 1, 3, 9$, which is not very helpful. But if we assume that $n_3 = 4$, we can consider the action of G on the 4 Sylow 3-subgroups by conjugation, giving a non-trivial homomorphism $f : G \to S_4$. But we immediately note that $72 \nmid 4! = |S_4|$, whence $\ker f$ must be non-trivial, and so a normal subgroup in G. Hence G is not simple.

27 Fri. 30/11/18 – the "finding simple groups" program

27.1 Strategies to prove $|G| = n$ is not simple

(1) *Sylow's theorem might tell you $n_p = 1$ for some $p \mid |G|$.*

(2) *Count elements.*

This works best when $|G| = pm$ with $(p, m) = 1$ and Sylow gives a large $n_p = m$.

It is harder to use when $|G| = p^a m$ with $a > 1$. It can happen that two Sylow p-subgroups $H \neq H'$ exist, with $H \cap H' \neq \{1\}$.

(3) *Look for group actions on small sets.*

Lemma: if a simple group G acts non-trivially on a set of size k and $G \not\simeq \mathbb{Z}/2\mathbb{Z}$, then $|G| \mid k!/2$.

Proof: we get a homomorphism $f : G \to S_k$, with $\ker f \neq G$ because the action is not trivial, but then $\ker f = \{1\}$, whence $|G| \mid k!$. Now consider the composite $G \to S_k \to S_k/A_k \simeq \mathbb{Z}/2\mathbb{Z}$, whose kernel cannot be $\{1\}$, for then $G \simeq \mathbb{Z}/2\mathbb{Z}$. But then it must be all of G, so $f(G) \subseteq A_k$, whence $|G| \mid k!/2$.

27.2 Groups of order 144

Note $144 = 2^4 \cdot 3^2$. Sylow analysis gives

- $n_3 = 1, 4, 16$
- $n_2 = 1, 3, 9$.

Now suppose that G is simple and of order 144. Since 144 divides neither $\frac{4!}{2}$ nor $\frac{3!}{2}$, from our previous consideration we can't have $n_3 = 4$ nor $n_2 = 3$. So we have $n_3 = 16$ and $n_2 = 9$.

Since we have a number of Sylow 3-subgroups, we consider two possible cases:

- For all $H \neq H'$ Sylow 3-subgroups, then $H \cap H' = \{1\}$. So G has $16 \cdot (9 - 1)$ elements of order 3 or 9, i.e. G has only 16 elements of order distinct from 3 and 9, which must then form a normal Sylow 2-subgroup, a contradiction.
- There is a pair of Sylow 3-subgroups $H \neq H'$ with non-trivial intersection. Then $|H \cap H'| = 3$. Consider $N = \mathrm{N}_G(H \cap H')$. We note that, since $H \simeq H' \simeq \mathbb{Z}/3\mathbb{Z}$, they are abelian, so $H \cap H' \trianglelefteq H, H'$, whence $H, H' \subseteq N$, i.e. $N \neq \{1\}$. Then either

  Subcase (a): $N = G$, so $H \cap H'$ is normal in G, a contradiction.

  Subcase (b): $N \neq G$, but $N \neq \{1\}$, so $[G : N] = 2$ or 4. We let G act on the cosets G/N, which by our lemma gives $|G| \mid 4!$, a contradiction.

27.3 Groups of order 60

28 Mon. 03/12/18 – finding more simple groups

28.1 Groups of order 60 (cont'd)

28.2 But where are simple groups?

Here is the list of simple groups we know so far:

- $\mathbb{Z}/p\mathbb{Z}$, for p prime (the only abelian simple groups); and
- A_n for $n \geq 5$.

:(

Simple groups seem sparse, since $|A_n| = \frac{n!}{2}$ grows very fast. For instance, $|A_5| = 60$ and $|A_6| = 360$, so we might ask: *is there any non-abelian simple group in between these two orders?* The answer is **Yes**.

Theorem 28.1. *For $n < 168 = 2^3 \cdot 3 \cdot 7$, and $n \neq 60$, there are no non-abelian simple groups of order n.*

(The punchline is that there *is* a non-abelian simple group of order 168, as we shall show next class.)

We better keep track of group orders for which we know for sure there are no simple groups.

Lemma 28.2. *There are no non-abelian simple groups of orders as follows, for p, q, l distinct primes and m odd;*

- *p^n, for it has non-trivial center; $x \in \mathrm{Z}(G)$ can be chosen to have order p by Cauchy's.*
- *pq, as per our work in class.*
- *p^2q, pql and $2m$, by this week's homework.*
- *$3p^n$, $4p^n$ and $8p$, as we shall show.*

29 Wed. 05/12/18 – simplicity of $\mathrm{PSL}_2(\mathbb{F}_p)$

We will add another group to our list of simple groups.

—

30 Midterm I review

(...)

31 Midterm II review

Things to know:

(1) Quotient groups and the first isomorphism theorem. (it can't hurt to be aware of the 2nd and 3rd isomorphism theorems but they are less important than the 1st!)

(2) Group actions:

   (a) Giving an action of a grup G on a set X is the same as giving a homomorphism $G \to S_X$.

   (b) Orbits, stabilizers, and the orbit-stabilizer theorem.

   (c) Some terminology for group actions: faithful and transitive actions, the kernel of a group action.

(3) Conjugation:

   (a) Conjugacy classes are the orbits, centralizers are the stabilizers.

   (b) Conjugacy classes for S_n.

(4) Simple groups, A_n is simple for $n \geq 5$.

Nothing about Sylow's theorems!

Here are some practice problems:

(1) True or false:

   (a) If G is a group with an abelian normal subgroup $H \subseteq G$ such that G/H is abelian, then G is abelian.

   Answer. False. For example, consider the subgroup of rotations in D_{2n}. □

   (b) If G is a cyclic group, then for any subgroup $H \subset G$, G/H is also cyclic.

   Answer. False. □

   (c) S_n is a simple group for $n \geq 5$.

   Answer. False. □

   (d) If $\phi : G \to H$ is a homomorphism then $\mathrm{im}(\phi)$ is a normal subgroup of H.

   Answer. False. □

   (e) If $K \subseteq H \subseteq G$ are subgroups and K is normal in G, then K is normal in H.

   Answer. False. □

   (f) Let G be a group. Then $\{(g, g) \mid g \in G\} \subset G \times G$ is a normal subgroup.

   Answer. False. □

   (g) Any two reflections in the Dihedral group D_{2n} for $n \geq 3$ are conjugate.

   Answer. False. □

(h) If G_1 and G_2 are groups then $\mathrm{Z}(G_1 \times G_2) = \mathrm{Z}(G_1) \times \mathrm{Z}(G_2)$.

Answer. False. □

(i) There are only finitely many groups up to isomorphism which can act transitively on a set with 7 elements.

Answer. False. □

(j) There are only finitely many groups up to isomorphism which can act faithfully on a set with 7 elements.

Answer. False. □

(2) Prove that

$$(\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) / \langle(\overline{3}, \overline{2})\rangle \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$$

Proof. Consider the map

$$\begin{aligned} \varphi : (\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) &\to \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \\ (\overline{x}, \overline{y}) &\mapsto (\overline{x}, 2\overline{x} + \overline{y}). \end{aligned}$$

This is clearly a homomorphism, since it's a linear combination of terms in the domain.

Furthermore, it is surjective: it is clear on the first coordinate, and for the second coordinate fixing $x = 0$ we have $0 \mapsto 0$, $1 \mapsto 1$, $2 \mapsto 2$, $3 \mapsto 3$, so it is surjective.

Finally, $(\overline{x}, \overline{y}) \in \ker(\varphi)$ iff $x \equiv 0 \pmod 3$, i.e. $x = 0, 3$, whence $y = 0$ and $y = 2$, so $\ker(\varphi) = \langle(\overline{3}, \overline{2})\rangle$.

Hence by the first isomorphism theorem, we get the result. □

(3) Prove that any finite group is isomorphic to a subgroup of A_n for some n.

Proof. Let G be a finite group. By Cayley's theorem, we have that G is isomorphic to a subgroup of S_n for some n. Now consider the injection

$$\begin{aligned} \phi : S_n &\to A_{n+2} \\ \sigma &\mapsto \begin{cases} (n+1\, n+2)\sigma & \text{if } \sigma \text{ is odd} \\ \sigma & \text{if } \sigma \text{ is even} \end{cases}. \end{aligned}$$

Hence S_n is isomorphic to some subgroup of A_{n+2}, and in particular G as well. □

(4) Write out the class equation for A_4 and D_8.

Solution. We recall that, since A_n is simple and the center of a group is always normal, necessarily $\mathrm{Z}(A_n) = \{1\}$. Thus

$$A_4 = [(1)]_{A_5} \coprod [(1\,2\,3)]_{A_4} \coprod [(1\,3\,2)]_{A_4} \coprod [(1\,2)(3\,4)]_{A_4}$$
$$|A_4| = 1 + 4 + 4 + 3.$$

For D_8, we have $\mathrm{Z}(D_8) = \{1, R_\pi\}$. □

(5) Let G be a finite group and let H be a proper subgroup. Show that $G \neq \bigcup_{g \in G} gHg^{-1}$.

(6) Let G be a group of order p^a for p prime. Prove that G has a subgroup of order p^b for all $b < a$. (*hint:* try to prove this by induction on a.)

Proof. By Cauchy's, we have an element $x \in G$ of order p. Then $G/\mathrm{N}_G(\langle x \rangle)$ has order p^{a-1}; we use the inductive hypothesis to get a subgroup K of order p^b.

Let $\overline{K}$ be the preimage of K under the quotient homomorphism; it corresponds to (…) □

(7) Let G be a group and suppose that the center $\mathrm{Z}(G)$ has index n in G. Show that every conjugacy class in G has size at most n.

(8) Let G be a group, and let $H \subseteq G$ be a subgroup. Consider the action of G on G/H given by $g \star aH = gaH$.

(a) Show that the stabilizer of the coset aH for this action is aHa^{-1}.

(b) Now suppose that H has index n in G. Show that $\bigcap_{g \in G} gHg^{-1}$ is a normal subgroup of G of index dividing $n!$.

(9) (a) Show that if a group G acts faithfully and transitively on a finite set X with n elements then $n \mid |G|$ and $|G| \mid n!$.

(b) Show that a group G cannot act faithfully and transitively both on a set of order 10 and a set of order 11.

(10) Let G be a finite simple group and suppose that G has a subgroup of index n. Show that $|G| \mid n!$.

(11) (a) Show that for $n \geq 5$, the only normal subgroups of S_n are $\{1\}$, A_n, and S_n.

(b) Show that for $n \geq 5$, any subgroup of $H \subset S_n$ of index n is isomorphic to S_{n-1}. (*hint:* consider the action of S_n on S_n/H, the set of left cosets of H. Also note that this is true for all n.)

(c) (just for fun) Remind yourself of Problem 8 on HW#5, and show that $\mathrm{PGL}_2(\mathbb{F}_5) \simeq S_5$.

32 Final review

32.1 Things to know

(1) The normalizer $N_G(H)$ is the stabilizer of H for the action of G on its subgroups by conjugation.

(2) Sylow's theorems, and most importantly what a Sylow subgroup is, Sylow subgroups exist, any two Sylow p-subgroups are conjugate, and what Sylow's 3rd theorem tells you about n_p.

(3) What to do when you have actually found some normal subgroups: if you have subgroups $H, K \subset G$ with $H \cap K = \{1\}$,
   (a) If both H, K are normal in G, then $H \times K \simeq HK$.
   (b) If H is normal in G then $H \rtimes_\phi K \simeq HK$, where $\phi(k)(h) = khk^{-1}$.
   (c) This will be especially useful if $|H||K| = G$, because then $G = HK$.

(4) Semidirect products: know what they are and what they are good for (point (b) above). In general, problems involving semidirect products can take a long time and require lots of computation, and so this limits what I can ask about them. Expect only short conceptual questions!

(5) Terminology about automorphisms: inner and outer automorphisms, and characteristic subgroups.

(6) Strategies for finding normal subgroups when Sylow's 3rd theorem alone fails:
   (a) Count elements in Sylow subgroups. This works especially well if $|G| = pm$, with $\gcd(p, m) = 1$, and Sylow tells you that $n_p = 1$ or m.
   (b) Find a non-trivial action of G on a small set, for example the Sylow p-subgroups if Sylow's theorem forces n_p to be small. (If a simple group G which is not isomorphic to $\mathbb{Z}/2\mathbb{Z}$ acts non-trivially on a set with n elements, then $|G|$ divides $n!/2$.)

(7) In general, you shouldn't feel the need to memorize the various things about classifications of groups of certain orders that we've proved in class or on the homework. However, it's not a bad idea to remember (or be able to quickly rediscover) these things:
   (a) If G is a group of order p^2, then either $G \simeq \mathbb{Z}/p\mathbb{Z}$ or $(\mathbb{Z}/p\mathbb{Z})^2$; in either case, G is always abelian.
   (b) If G is a group of order pq with $p > q$ primes, and if $p \not\equiv 1 \pmod{q}$, then G is cyclic. If $p \equiv 1 \pmod{q}$, then G is isomorphic to a non-abelian semidirect product $(\mathbb{Z}/p\mathbb{Z}) \rtimes (\mathbb{Z}/q\mathbb{Z})$. (In fact, there is only one such semidirect product up to isomorphism, assuming that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic.)

32.2 Practice problems

(1) Let G be a finite group.

(a) Let $K \subset G$ be a normal subgroup of order $|K| = p^a$ for some prime p. Show that for any Sylow p-subgroup $H \subset G$, we have $K \subset H$.

Proof. K is a p-subgroup of G, so by Sylow's second theorem we have $gKg^{-1} \subset H$. But K is furthermore normal, whence $K \subset H$. □

(b) Show that the intersection of all Sylow p-subgroups of G is normal in G.

Proof. By part (a), we have that $K \subseteq H$. Suppose there is some $h \in H$ with $h \notin K$. Then h is in every Sylow p-subgroup H_i of G, which can be obtained by conjugating a given Sylow p-subgroup H_0.
(…) □

(2) Let G be a finite group, let H be a Sylow p-subgroup, and let K be a normal subgroup of G. Show that $H \cap K$ is a Sylow p-subgroup of K. Give an example showing this is false in general if K is not normal.

Proof. We have $|G| = p^a m$ with $(p, m) = 1$, $|H| = p^a$, and $|K| = p^b m'$ with $(p, m') = 1$ and $b \leq a$.

From this, we immediately see by Lagrange's that $|H \cap K| = p^k$, for $k \leq b$. Our goal is to show that $k = b$, i.e. that $H \cap K$ is a Sylow p-subgroup of K.

We use Sylow's 2nd theorem to get that $H \cap K \subseteq H'$ for some Sylow p-subgroup H' of K.

Also, H' is a p-subgroup of G, so $gH'g^{-1} \subseteq H$ for some $g \in G$. Note that $gH'g^{-1} \subseteq K$ by K being normal. Hence, intersecting both sides by K gives $gH'g^{-1} \subseteq H \cap K$.

From these two inclusions we get that $|H \cap K| = |H'|$, i.e $H \cap K$ is a Sylow p-subgroup of K.

For a counterexample if K is not normal, (…). □

(3) How many elements of order 3 are there in S_6?

Proof. An element of order 3 in S_6 must be either a 3-cycle or a (3,3)-cycle. In the first case, there are $\frac{6 \cdot 5 \cdot 4}{3} = 40$ of them, and in the second case, there are $\frac{6!}{2!3^2} = 40$ of them, giving a total of 80 elements of order 3. □

(4) Let G and H be groups. Show that $\mathrm{Z}(G \times H) = \mathrm{Z}(G) \times \mathrm{Z}(H)$.

Proof. An element $(g, h) \in G \times H$ is in the center iff $(g, h)(a, b) = (a, b)(g, h)$ for all $(a, b) \in G \times H$ iff $ga = ag$ and $hb = bh$ for all $a \in G$ and all $b \in H$ iff $g \in \mathrm{Z}(G)$ and $h \in \mathrm{Z}(H)$. □

(5) (a) Show that $D_{4n} \simeq D_{2n} \times \mathbb{Z}/2\mathbb{Z}$ if and only if n is odd.

Proof. □

(b) Show that D_{2pn} is not isomorphic to D_{2n} for any n if p is an odd prime.

Proof. □

(6) (a) Describe $\mathrm{C}_{S_5}((1\,2\,3))$.

Proof. By the Orbit-Stabilizer theorem, we have

$$|\,\mathrm{C}_{S_5}((1\,2\,3))| = \frac{|S_5|}{|\text{orbit of } (1\,2\,3)|} = 3 \cdot 2$$

but since $(1\,2\,3)^k(1\,2\,3)(1\,2\,3)^{-k} = (1\,2\,3)$, the centralizer of $(1\,2\,3)$ immediately contains the three powers of $(1\,2\,3)$, and the same three powers together with the transposition $(4\,5)$. This exhausts the centralizer. □

(b) Describe $\mathrm{N}_{S_5}(\langle(1\,2\,3)\rangle)$.

Proof. We claim that $\mathrm{N}_{S_5}(\langle(1\,2\,3)\rangle) \simeq \mathrm{N}_{S_3}(\langle(1\,2\,3)\rangle) \times S_2$, whence $|\,\mathrm{N}_{S_5}(\langle(1\,2\,3)\rangle)| = (3 \cdot 2) \cdot 2 = 12$.
(?? structure of normalizer ??) □

(7) Show that if $H \times \{1\}$ and $\{1\} \times K$ are characteristic subgroups of $H \times K$, then $\mathrm{Aut}(H \times K) \simeq \mathrm{Aut}(H) \times \mathrm{Aut}(K)$. Give an example where $H \times \{1\}$ is not a characteristic subgroup of $H \times K$.

Proof. Fix any $\phi \in \mathrm{Aut}(H \times K)$. For any $(h,k) \in H \times K$, we have $\phi(h,k) = \phi((h,1)(1,k)) = \phi(h,1)\phi(1,k)$. Since $\phi(h,1) \in H \times \{1\}$ and $\phi(1,k) \in \{1\} \times K$ by these two subgroups being characteristic, we can associate automorphisms $\phi_H \in \mathrm{Aut}(H)$ and $\phi_K \in \mathrm{Aut}(K)$ to ϕ for which $\phi(h,1) = (\phi_H(h),1)$ and $\phi(1,k) = (1,\phi_K(k))$ for all $h \in H$ and $k \in K$.

This defines a map $\mathrm{Aut}(H \times K) \to \mathrm{Aut}(H) \times \mathrm{Aut}(K)$; furthermore, this map has an inverse defined as follows. For any $\phi_H \in \mathrm{Aut}(H)$ and $\phi_K \in \mathrm{Aut}(K)$, form the automorphism $\phi \in \mathrm{Aut}(H \times K)$ given by $\phi(h,k) = (\phi_H(h), \phi_K(k))$. □

(8) Let G be an abelian group acting faithfully and transitively on a set X. Show that for any $x \in X$, the stabilizer $\mathrm{Stab}_G(x)$ is trivial.

Proof. Suppose that there exists some $x \in X$ for which $\mathrm{Stab}_G(x)$ is not trivial, i.e. for which there is some $g \in \mathrm{Stab}_G(x)$ with $g \neq 1$. Fix $y \neq x \in X$; since the action is transitive, we have some $h \in G$ such that $hx = y$. Then $gy = (gh)x = (hg)x = hx = y$, i.e $g \in \mathrm{Stab}_G(y)$. Since y was arbitrary, we have that $gx = x$ for all $x \in X$, i.e. the kernel of the homomorphism given by this action is not trivial, which contradicts the assumption that the action was faithful. □

(9) Recall that $\mathrm{PSL}_2(\mathbb{F}_5) \simeq A_5$. Show that there is no isomorphism $\mathrm{PSL}_2(\mathbb{F}_p) \simeq A_n$ for $p > 5$ prime and $n > 5$.

Proof. □

(10) Let G be a group and let $g \in G$ be such that $\langle g \rangle$ is normal in G. Show that $\langle g^n \rangle$ is also normal in G for any n.

Proof. Recall that if $H \trianglelefteq G$ and $K \subseteq H$ is characteristic in H, then $K \trianglelefteq G$.

For this particular case, any automorphism ϕ of G is determined on $\langle g \rangle$ by $\phi(g) = g^k$. Then, for any $g^{rn} \in \langle g^n \rangle$, we have $\phi(g^{rn}) = g^{krn} \in \langle g^n \rangle$, whence $\langle g^n \rangle$ is characteristic in $\langle g \rangle$. The claim follows.

Or, alternatively: since $\langle g^n \rangle$ is the unique subgroup of a particular order of $\langle g \rangle$, then $\phi(\langle g^n \rangle) = \langle g^n \rangle$. □

(11) Let G be a group of order $231 = 3 \cdot 7 \cdot 11$. Show that $\mathrm{Z}(G)$ contains an element of order 11.

Proof. Sylow analysis gives $n_{11} = 1$. Consider the action of G on the unique Sylow 11-subgroup H_{11} by conjugation, i.e. $ghg^{-1} = h'$ for all $g \in G$, $h \in H_{11}$. This gives a homomorphism $f : G \to \mathrm{Aut}(H_{11}) \simeq (\mathbb{Z}/11\mathbb{Z})^\times$.

By the 1st isomorphism theorem, we have that $\frac{|G|}{|\ker f|}$ divides $|\,(\mathbb{Z}/11\mathbb{Z})^\times\,| = 10$, but this is impossible unless $[G : \ker f] = 1$, i.e. $\ker f = G$, whence $ghg^{-1} = h$ for all $g \in G$ and $h \in H_{11}$. In particular, this implies that $h \in \mathrm{Z}(G)$, and since H_{11} is cyclic of order 11 it contains an element of order 11, which as noted is also in $\mathrm{Z}(G)$. □

(12) Show that there are no simple groups of the following orders:

(a) $9045 = 3^2 \cdot 5 \cdot 67$.

Proof. Sylow analysis gives $n_{67} = 1$. □

(b) $1960 = 2^3 \cdot 5 \cdot 7^2$.

Proof. Sylow analysis gives $n_7 = 1$ or 8. Suppose that $n_7 = 8$, and consider the action of G on the Sylow 7-subgroups of G. We have a homomorphism $G \to S_8$, forcing $|G| \mid 8!/2$, i.e. $2^3 \cdot 5 \cdot 7^2 \mid 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3$, which is impossible. □

(c) $380 = 2^2 \cdot 5 \cdot 19$.

Proof. Sylow analysis gives $n_{19} = 1$ or 20 and $n_5 = 1$ or 76. Assuming that neither of them is one, we count $76 \cdot (5-1) + 20 \cdot (19-1) = 664$ elements in G of order either 5 or 19, but $|G| = 380$, giving a contradiction. □

(d) $100000 = 2^4 \cdot 5^4$.

Proof. Sylow analysis gives $n_5 = 1$ or 16. Suppose that $n_5 = 16$; let G act on the Sylow 5-subgroups by conjugation, giving a homomorphism $G \to S_{16}$, whence $|G| \mid 16!/2$. However, notice that $|G|$ contains 4 factors of 5, while the right side contains only 3 (corresponding to 15, 10 and 5); this is a contradiction. □

(13) Show that a group of order 63 must contain an element of order 21.

Proof. Write $63 = 3^2 \cdot 7$. Sylow analysis gives $n_7 = 1$ and $n_3 = 1$ or 7. Hence we have a normal Sylow 7-subgoup H_7 and a number of Sylow 3-subgroups, for instance H_3. By our semidirect product master theorem, we get that $H_7 \rtimes_\phi H_3 \simeq H_7 H_3 = G$. Writing $H_7 = \langle x \rangle$, we are looking for an element $y \in H_3$ of order 3 which commutes with x, because then $\operatorname{ord}(xy) = \operatorname{ord}(x)\operatorname{ord}(y) = 21$.

More explicitly, we want some $y \in H_3$ for which $yxy^{-1} = x$. This is equivalent to asking that $\phi(y) \in \operatorname{Aut}(H_7)$ be the identity. But $\operatorname{Aut}(H_7) \simeq \mathbb{Z}/6\mathbb{Z}$, so our automorphism map is $f : H_3 \to \mathbb{Z}/6\mathbb{Z}$, which gives $|\ker f| = 3$ or 9 (and not 1 because $|H_3| > 6$).

In either case, we can choose $y \in \ker f$ of order 3, which gives $yxy^{-1} = x$ and thus $\operatorname{ord}(xy) = 21$. □

(14) Let G be a finite simple group containing an element of order 21. Show that any proper subgroup of G has index at least 10.

Proof. □

(15) (a) Let G be a finite group, and let p be the largest prime dividing the order of G. Prove that G does not act faithfully on a set with less than p elements.

Proof. Write $|G| = p^k m$, with p the largest prime factor of the order of G. Suppose that G acts on a set X with $|X| = n < p$. This gives a homomorphism $f : G \to S_n$. By Sylow's theorem, we have a Sylow p-subgroup $H_p \subseteq G$. Then $|f(H_p)| \mid p^k$ and $|f(H_p)| \mid n < p$, which is impossible unless $H_p \subseteq \ker f$, i.e. the action is *not* faithful. □

(b) Let G be a finite simple group, and suppose that G has a subgroup H of index p. Show that p must be the largest prime dividing the order of G.

Proof. Let G be a finite simple group with a subgroup H of index p, and suppose that there is a prime $q > p$ dividing G.

Consider the action of G on the p cosets of G/H. Since $q > p$, we apply (a) and get that this action cannot be faithful, i.e. its associated homomorphism has non-trivial kernel $\subseteq G$, which implies that G is not normal, a contradiction. □

(c) With the notation as in the last part, show that the set of conjugates of H in G, i.e. $\{gHg^{-1} \mid g \in G\}$, has size p.

Proof. □

(16) Let G be a group with $\mathrm{Z}(G) = \{1\}$. Show that $\mathrm{Z}(\mathrm{Aut}(G)) = \{1\}$.

Proof. Suppose that some $\phi \in \mathrm{Aut}(G)$ commutes with all automorphisms. In particular, it commutes with all $\psi_g \in \mathrm{Inn}(G)$, i.e. $\psi_g \circ f(h) = f \circ \psi_g(h)$ for all $h \in G$, so

$$\begin{aligned} g\phi(h)g^{-1} &= \phi(g)\phi(h)\phi(g)^{-1} \\ \phi(g)^{-1}g\phi(h)g^{-1}\phi(g) &= \phi(h). \end{aligned}$$

Since f is an automorphism, the equality above can be rewritten as

$$\left(\phi(g)^{-1}g\right) x \left(g^{-1}\phi(g)\right) = x$$

for all $x \in G$, i.e. $\phi(g)^{-1}g \in \mathrm{Z}(G)$, a contradiction. □

(17) Let H be a subgroup of S_n generated by two 3-cycles. Show that H is isomorphic to one of $\mathbb{Z}/3\mathbb{Z}$, $(\mathbb{Z}/3\mathbb{Z})^2$, A_4, or A_5.

Proof. Let $H = \langle (a\,b\,c)(d\,e\,f) \rangle$. We consider the multiple possible cases:

- *Disjoint cycles, or same cycle:* then $|H| = 3$, i.e. $H \simeq \mathbb{Z}/3\mathbb{Z}$.
  (…)

□

(18) Show that S_{20} has a subgroup isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{10}$, and that S_n has no subgroup isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{10}$ for $n < 20$.

Proof. Consider $H = \langle (1\,2)(3\,4)\cdots(19\,20) \rangle$. □

(19) View S_n as the subgroup of S_{n+1} of permutations fixing $n+1$. Show that if $S_n \subseteq H \subseteq S_{n+1}$ is a subgroup, then either $H = S_n$ or $H = S_{n+1}$.

Proof. □

(20) (a) Let H be a group. Show that $f : H \to H$ given by $f(h) = h^{-1}$ is an automorphism of H if and only if H is abelian.

Proof. ($\Longrightarrow$) Since f is an automorphism, we have $f(g^{-1}h^{-1}) = f(g^{-1})f(h^{-1})$, whence $(g^{-1}h^{-1})^{-1} = (g^{-1})^{-1}(h^{-1})^{-1}$, i.e. $hg = gh$. Hence H is abelian.
($\Longleftarrow$) We have $f(gh) = (gh)^{-1} = (hg)^{-1} = g^{-1}h^{-1} = f(g)f(h)$, so f is a homomorphism. Furthermore, given $h \in H$, we have $f(h^{-1}) = h$, so f is surjective. Since f maps onto itself, we immediately get that f is an automorphism. □

(b) Suppose that H is abelian. Let $K = \langle x \rangle$ be a cyclic group of order 2. Let $\phi : K \to \mathrm{Aut}(H)$ be defined by $\phi(x) = f$. Show that for any $h \in H$, the element $(h, x) \in H \rtimes_\phi K$ has order 2.

Proof. We have

$$(h, x)(h, x) = (h\phi(x)(h), x^2) = (hf(h), 1) = (hh^{-1}, 1) = (1, 1).$$

□