Fall 2023

Groups

1 Definition and first examples

Definition 1.1. A *group* is a set G with a binary operation (multiplication) $\cdot : G \times G \to G$ satisfying the axioms:

1. the group operation is associative: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
2. there exists an identity element $e \in G$ such that $a \cdot e = e \cdot a = a$ for any $a \in G$
3. for each $a \in G$ there exists the inverse element $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Definition 1.2. A group G is *finite* if the set G is finite.

Definition 1.3. A group G is *abelian* (commutative) if $a \cdot b = b \cdot a$ for all $a, b \in G$.

Example 1.4. The integers form a group with respect to addition: $(\mathbb{Z}, +)$. This is an infinite abelian group with $e = 0$.

Definition 1.5. If G is finite as a set, then the *order of the group* G is the number of elements in G. Notation: $|G|$.

Example 1.6. The (counterclockwise) rotations in $\mathbb{R}^2$ around a point by multiples of $2\pi/n$ form a group with respect to compositions with e being the rotation by 0 angle. This is the cyclic group of order n, denoted C_n. This is an abelian group of order n.

Example 1.7. Consider the congruence classes of integers modulo n: $\{[0]_n, [1]_n, \dots [n-1]_n\}$. These are all the possible remainders of the division by n. They form a group with respect to addition and the identity element given by $[0]_n$. This is an abelian group of order n.

Notation 1.8. We will often write 1 (or 0 for groups written additively) instead of e for the identity element of the group, if there is no risk of confusion. We will often omit $\cdot$ and assume that $ab = a \cdot b$ means the product of a and b in the group.

Definition 1.9. *Generators* of a group G form a subset $S \subset G$ such that any element of G can be written as a product of the elements in S.

Definition 1.10. Any equation satisfied by the generators is a *relation* in G.

Definition 1.11. A *presentation of G in terms of generators and relations* is the expression

$$\langle S \mid R_1, R_2, \dots R_k \rangle$$

where S is a set of generators of G and $R_1, R_2, \dots R_k$ are the relations satisfied by the elements in S such that any other relation follows from these.

Example 1.12. Presentation in terms of generators and relations of the cyclic group C_n:

$$C_n = \langle q \mid q^n = 1 \rangle$$

Definition 1.13. Let g be an element in the group G. The smallest positive integer n such that $g^n = 1$, if it exists, is called the *order of the element g in G* and denoted $o(g)$. If there is no such integer, then we say that g is of infinite order (this implies that the group G is infinite).

Example 1.14. Consider the cyclic group $C_{12} = \langle q \mid q^{12} = 1 \rangle$ (You can think of q as the rotation in $\mathbb{R}^2$ around the origin by $2\pi/12$). Then $o(q) = 12$. We also have $o(q^2) = 6$ and $o(q^4) = 3$.

2 Group homomorphisms. Subgroups and normal subgroups.

Definition 2.1. A map $\phi : G \to H$ between two groups is a *group homomorphism* if

$$\phi(x \cdot_G y) = \phi(x) \cdot_H \phi(y)$$

for any $x, y \in G$.

Remark 2.2. If $\phi : G \to H$ is a group homomorphism, then $\phi(1_G) = 1_H$ and $\phi(x^{-1}) = \phi(x)^{-1}$ for any $x \in G$.

Definition 2.3. A *group isomorphism* is a homomorphism $\phi : G \to H$ that is a bijection between the sets G and H.

Definition 2.4. A *group endomorphism* is a homomorphism $\phi : G \to G$. A *group automorphism* is an isomorphism $\phi : G \to G$.

Example 2.5. The map

$$\phi : C_n \to \mathbb{Z}/n\mathbb{Z}, \quad \phi(q) = [1]_n$$

is an isomorphism between the cyclic group of rotations by multiples of $2\pi/n$ and the group of integers modulo n with respect to addition. Here q is a generator of C_n, and $[1]_n$ is the congruence class of 1 modulo n.

Definition 2.6. The *kernel* of a homomorphism $\phi : G \to H$ is the set of all elements $g \in G$ such that $\phi(g) = 1_H$: $\text{Ker}\phi = \{g \in G \ : \phi(g) = 1\}$. The image of a homomorphism $\phi : G \to H$ is the set $\text{Im}\phi = \{h \in H \mid \exists g \in G \ : \phi(g) = h\}$.

Remark 2.7. An endomorphism $\phi : G \to G$ is an automorphism if and only if $\text{Ker}\phi = \{1\}$.

Remark 2.8. If G is presented in terms of generators and relations, to check if a given map $\phi : G \to H$ is a group homomorphism, it suffices to check that the images of the generators of G in H satisfy the relations for the generators in G.

Example 2.9. Let $C_6 = \langle q \mid q^6 = 1\rangle$ and $C_4 = \langle t \mid t^4 = 1\rangle$. The map

$$\phi : C_6 \to C_4, \quad \phi(q) = t^2$$

is a group homomorphism. We have $\text{Im}\phi = \{1, t^2\}$, and $\text{Ker}\phi = \{1, q^2, q^4\}$.

Definition 2.10. A *subgroup* $H \subset G$ is a nonempty subset of G that forms a group with respect to the group operation in G. In particular, $1 \in H$ and for any $a, b, \in H$, we have $a \cdot b \in H$.

Example 2.11. Consider the cyclic group C_{12}. The elements $\{1, q^3, q^6, q^9\}$ form a subgroup in C_{12}.

Definition 2.12. A subgroup $H \subset G$ is *normal* if $ghg^{-1} \in H$ for any $g \in G, h \in H$. Notation: $H \lhd G$.

Proposition 2.13. *If G is abelian, any subgroup is normal in G: $H \subset G \implies H \lhd G$.*

Proposition 2.14. *Let $\phi : G \to H$ be a group homomorphism. Then*

1. *The image of ϕ is a subgroup in H: $\phi(G) \subset H$.*
2. *The kernel of ϕ is a normal subgroup in G: $\text{Ker}\phi \lhd G$.*

Proof: Practice Problem Set.

3 The dihedral group D_n.

Definition 3.1. The *dihedral group* D_n, $n \geq 3$ is the group of rigid symmetries of a flat regular n-gon. The group operation is composition.

Proposition 3.2. *The dihedral group D_n is a non-abelian group of order $2n$. It has the following presentation in generators and relations:*

$$D_n = \langle r, s \mid r^n = 1,\ s^2 = 1,\ srs = r^{-1}\rangle.$$

You can think of r as a rotation of the regular n-gon around its center by the angle $2\pi/n$ and of s as the reflection about the straight line passing through one of the vertices of the regular n-gon.

Proposition 3.3. *A complete list of elements of D_n in terms of generators and relations is given by the list*

$$D_n = \{1, r, r^2, \ldots r^{n-1}, s, sr, \ldots sr^{n-1}\}.$$

For proofs of these statements, and discussion of further properties of dihedral groups see the resource "Dihedral groups" available on the Moodle page of the course.

Exercise 3.4. The subset $R = \{1, r, \dots r^{n-1}\}$ forms a subgroup in the dihedral group D_n for any $n \geq 3$. Use the relations in D_n to check that this subgroup is normal: $R \lhd D_n$.

Example 3.5. The subset $H = \{1, s\} \subset D_n$ forms a subgroup in the dihedral group D_n (for any $n \geq 3$). But H is not normal in D_n, because we have $rsr^{-1} = sr^{-2} \notin H$. (Here we used the relations $srs = r^{-1}$, $s^2 = 1 \implies rs = sr^{-1}$.

4 Cosets. Lagrange's theorem.

Definition 4.1. Let $H \subset G$ be a subgroup. A *left coset* with respect to H in G is the subset of element of G defined as follows:

$$gH = \{gh, h \in H\}.$$

Similarly, a right coset with respect to H in G is the subset of element of G defined as follows: $Hg = \{hg, h \in H\}$. In what follows we will use only left cosets and often omit the word "left".

Example 4.2. Consider the subgroup $H = \{1, s\}$ in the dihedral group $D_4 = \langle r, s \mid r^4 = 1,\ s^2 = 1, srs = r^{-1}\rangle$. There are 4 distinct left H-cosets in D_4:

$$1H = \{1, s\}, \quad rH = \{r, rs\}, \quad r^2H = \{r^2, r^2s\}, \quad r^3H = \{r^3, r^3s\}.$$

Note that the order (number of elements) of each H-coset is equal to the order of H, and that D_4 is the union of all its left H-cosets:

$$D_r = (1H) \cup (rH) \cup (r^2H) \cup (r^3H).$$

Exercise 4.3. Check that any other left coset in D_4 coincides with one of the cosets listed above. For example, the coset $srH = \{sr,\ srs\} = \{r^{-1}s,\ r^{-1}\} = \{r^3s,\ r^3\} = r^3H$.

Proposition 4.4. *Let H be a subgroup of G.*

1. *Two cosets xH and yH are either equal, or disjoint.*
2. *Any element $g \in G$ belongs to an H-coset.*
3. *If H is finite, $|xH| = |yH|$ for any $x, y \in G$.*

Proof:

1. Suppose $xH \cap yH \neq \emptyset$. Then there exists an element $z \in xH \cap yH$ such that $z = xh_1 = yh_2$, which implies $x = yh_2h_1^{-1} \in yH$. Suppose $t \in xH$, then $t = xh_3 = yh_2h_1^{-1}h_3 \in yH$. Therefore, the coset xH is a subset of the coset yH. By the same argument the opposite inclusion holds. This proves $xH = yH$.
2. Let $g \in G$. Then $g \in gH$ since the subgroup H contains the neutral element.
3. Let H be a finite subgroup of G, and $g \in G$. The map $f : H \to gH$ is a bijection: suppose that $gh_1 = gh_2$. Then $(g^{-1}g)h_1 = (g^{-1}g)h_2$ implies $h_1 = h_2$. The map is surjective by the definition of the left coset. Therefore the number of elements in each left H-coset is equal to $|H|$.

Theorem 4.5. *(Lagrange's Theorem). Let G be a finite group, and $H \subset G$ a subgroup. Then the order of H divides the order of G.*

Proof: Lecture 3.

Definition 4.6. In the conditions of Lagrange's theorem, the number $[G : H] = |G|/|H|$ is called the *index of H in G*. It equals to the number of left H-cosets in G.

Corollary 4.7. *In a finite group, the order of any element divides the order of the group.*

Proof: Let G be a finite group, and $g \in G$. Then the powers of g form a subgroup: $\{1, g, g^2, \dots g^{n-1}\} = H \subset G$, where n is the order of g. By Lagrange's theorem, $n = |H|$ divides $|G|$.

Corollary 4.8. *If G is a finite group, and $H \subset K \subset G$ nested subgroups, then*

$$[G : H] = [G : K][K : H].$$

Proof: By Lagrange's theorem we have $[G:H] = \frac{|G|}{|H|}$ for any subgroup $H \subset G$ of a finite group G. Then we have $[G:K][K:H] = \frac{|G|}{|K|}\frac{|K|}{|H|} = \frac{|G|}{|H|} = [G:H]$.

Corollary 4.9. *Let G be a finite group, and $g \in G$ an element. Then $g^{|G|} = 1$.*

Proof: Let n be the order of $g \in G$. By Corollary 4.7 n divides $|G|$. Then we have $|G| = nk$ for an integer k, and $g^{|G|} = g^{nk} = (g^n)^k = 1^k = 1$.

Corollary 4.10. *Let G be a finite group of prime order, $|G| = p$. Then G is cyclic (= there exists $x \in G$ such that $G = \{1, x, x^2, \dots x^{p-1}\}$.)*

Proof: PS 3.

Example 4.11. Lagrange's theorem allows us to classify groups of order 4. Let $|G| = 4$. If G contains an element x of order 4, then G is cyclic of order 4. Indeed, it contains then all powers of x from 0 to 3: $\{1, x, x^2, x^3\}$. Since $|G| = 4$, this is a complete list of elements of the group. Now suppose G does not contain an element of order 4. Then it contains the identity element and each of the three remaining elements must have order 2 (dividing the order of the group). If $a, b \in G$ with $a^2 = b^2 = 1$, then G also contains $ab : (ab)^2 = 1$. The last equation implies $(ab)^{-1} = ba = ab$, therefore the group is abelian and we have $G = \langle a, b \mid a^2 = b^2 = 1, ab = ba\rangle$. This group is called *the Klein group*.

Similarly, Lagrange's theorem allows to classify all groups of order 6 (see PS4).

5 Applications of Lagrange's theorem in arithmetic.

Definition 5.1. The *group of units* in $\mathbb{Z}/n\mathbb{Z}$ is the group of all invertible elements in $\mathbb{Z}/n\mathbb{Z}$ with respect to multiplication. It is denoted $((\mathbb{Z}/n\mathbb{Z})^*, \cdot)$.

Example 5.2. We have: $((\mathbb{Z}/6\mathbb{Z})^*, \cdot) = \{[1]_6, [5]_6\}$.
$((\mathbb{Z}/7\mathbb{Z})^*, \cdot) = \{[1]_7, [2]_7, [3]_7, [4]_7, [5]_7, [6]_7\}$.

Proposition 5.3. *Let $[a]_n \in \mathbb{Z}/n\mathbb{Z}$, $[a]_n \neq [0]_n$. Then $[a]_n$ is a unit in $\mathbb{Z}/n\mathbb{Z}$ if and only if $\gcd(a, n) = 1$. In particular, $|((\mathbb{Z}/n\mathbb{Z})^*, \cdot)| = \varphi(n)$, where $\varphi(n)$ is the Euler's totient function of n.*

Proof: Let $[b]_n \in \mathbb{Z}/n\mathbb{Z}$ be such that $[a]_n[b]_n = [1]_n$. This means that there exists $k \in \mathbb{Z}$ such that $ab = kn + 1$. Such $b, k \in \mathbb{Z}$ exist if and only if $\gcd(a, n) = 1$ by Bezout's theorem.

Theorem 5.4. *(Fermat's Little Theorem (FLT)). Let p be a prime, and $a \in \mathbb{Z}$ such that p does not divide a. Then*

$$a^{p-1} \equiv 1 \pmod p.$$

Proof: Consider the multiplicative group $((\mathbb{Z}/p\mathbb{Z})^*, \cdot)$. It has $\varphi(p) = p - 1$ elements. Since p does not divide a, we have $a \equiv t \pmod p$, where $t \in \{1, 2, \dots p-1\}$, so a is an element in the group $G = ((\mathbb{Z}/p\mathbb{Z})^*, \cdot)$. By Lagrange's theorem, we have $[a]_p^{|G|} = [1]_p$ in this group, therefore $[a]_p^{p-1} = [1]_p$. This means $a^{p-1} = mp + 1$ for some integer m, or equivalently $a^{p-1} \equiv 1 \pmod p$.

Remark 5.5. For any $a \in \mathbb{Z}$, p a prime, we have $a^p \equiv a \pmod p$. Proof: exercise.

Theorem 5.6. *(Euler's Theorem). Let $a, n \in \mathbb{Z}^+$, such that $\gcd(a, n) = 1$. Then*

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

where $\varphi(n)$ is Euler's totient function of n.

Proof: The group $G = ((\mathbb{Z}/n\mathbb{Z})^*, \cdot)$ has $\varphi(n)$ elements. We have $[a]_n \in G$ if and only if $\gcd(a, n) = 1$. Then by Lagrange's theorem, $[a]_n^{|G|} = [1]_n$, which is equivalent to $a^{\varphi(n)} \equiv 1 \pmod n$.

Example 5.7. Find $1 \leq x \leq 6$ such that $5^{601} \equiv x \pmod 7$. By FLT we have $5^6 \equiv 1 \pmod 7$, therefore $5^{600} \equiv 1 \pmod 7$, and $5^{601} \equiv 5 \pmod 7$, so $x = 5$.

Remark 5.8. For a prime p, the group $((\mathbb{Z}/p\mathbb{Z})^*, \cdot)$ is cyclic of order $p-1$. For a proof see the file "units-mod-p.pdf" in the Resources.

6 Quotient group.

Proposition 6.1. *Let G be a group, and $N \lhd G$ a normal subgroup. The set of left N-cosets in G is a group under the operation*

$$(xN)(yN) = (xyN).$$

Proof: $(xN)(yN) = (x(yy^{-1})N)(yN) = xy(y^{-1}Ny)N = xyN$. The last equality follows because N is normal: for any $n \in N$ we have $y^{-1}ny = n' \in N$. We need to check that the product is well-defined (does not depend on the choice of a representative of the left coset). Suppose $xN = uN$ and $yN = vN$. Then we have $xyN = uvN$ if and only if $(uv)^{-1}xy \in N$. We compute:

$$(uv)^{-1}xy = v^{-1}(u^{-1}x)y = v^{-1}n_1y = v^{-1}y(y^{-1}n_1y) = v^{-1}yn_2 = n_3n_2 \in \mathbb{N}.$$

Here we used that $u^{-1}x \in N$, $v^{-1}y \in N$ and $y^{-1}n_1y \in N$. Therefore the product is well defined.

It is easy to see that $1N$ is the neutral element and $x^{-1}N$ is the inverse element for xN for any $x \in G$.

Definition 6.2. Let $N \lhd G$. Then the group of left N-cosets in G is called the *quotient group* and denoted G/N.

Example 6.3. The dihedral group D_n has a normal subgroup of all rotations $\{1, r, \dots r^{n-1}\}$, isomorphic to the cyclic group C_n. The quotient group D_n/C_n is the cyclic group of order 2: $D_n/C_n = \{1C_n, sC_n\}$.
Note that the subgroup $H = \{1, s\} \in D_n$ is not normal (see Example 3.5), so that we cannot define a product on the set of left H-cosets in D_n.

Recall that if $\phi : G \to H$ is a group homomorphism, then $\mathrm{Ker}\phi \lhd G$ is a normal subgroup and $\mathrm{Im}\phi \subset H$ is a subgroup (Proposition 2.14). You can check directly that $\mathrm{Im}\phi$ is a subgroup of H (it contains the neutral element, and is closed with respect to multiplication and taking inverses, which follows from the definition of a group homomorphism). Similarly you can check that $\mathrm{Ker}\phi$ is a subgroup in G. Let us check that $\mathrm{Ker}\phi$ is a *normal* subgroup in G. Let $k \in \mathrm{Ker}\phi$ and $g \in G$. Then by definition $\phi(k) = 1_H$. By definition of a group homomorphism we have

$$\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g)^{-1} = \phi(g)1_H\phi(g)^{-1} = 1_H.$$

Therefore, $gkg^{-1} \in \mathrm{Ker}\phi$ as well, and $\mathrm{Ker}\phi \lhd G$.

Proposition 6.4. *Let $\phi : G \to H$ be a group homomorphism. Then $G/\mathrm{Ker}\phi \simeq \mathrm{Im}\phi$.*

Proof: Let $K = \mathrm{Ker}\phi \lhd G$. We define $\vartheta : G/K \to H$ by setting $\vartheta(gK) = \phi(g)$ for any $g \in G$. Then we can check that (1) ϑ is well defined (does not depend on the choice of the representative), (2) ϑ is a group homomorphism, (3) the image of ϑ is $\phi(G) \subset H$, and (4) $\vartheta : G/K \to H$ is injective.

Example 6.5. Fix $n \in \mathbb{N}^*$ and let $\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ by $\phi(x) = x \pmod n$. Then ϕ is a homomorphism with respect to addition: $\phi(x + y) = x(\mathrm{mod}\ n) + y(\mathrm{mod}\ n) = \phi(x) + \phi(y)$.
We have $\mathrm{Ker}\phi = \{n\mathbb{Z}\}$, and $\mathrm{Im}\phi = \mathbb{Z}/\mathrm{Ker}\phi = \mathbb{Z}/n\mathbb{Z} = \{[0]_n, [1]_n, \dots [n-1]_n\}$.

7 The symmetric group S_n

Definition 7.1. Let G be a finite group and E a finite set. We say that *G acts on E* (by permutations) if for all $x \in E$ and $g \in G$ the element $g \cdot x \in E$ is defined, such that

1. $1 \cdot x = x \quad \forall x \in E$,
2. $(g_1g_2) \cdot x = g_1 \cdot (g_2 \cdot x) \quad \forall g_1, g_2 \in G, \quad \forall x \in E$.

Definition 7.2. Let G act on the set E. The *orbit* of $x \in E$ is the set

$$\mathrm{Orb}_x = \{g \cdot x,\ g \in G\}.$$

The orbits of size 1 are called the *fixed points* of the action.

Definition 7.3. The *symmetric group* of order n is the group of all permutations (bijective maps) of $n \geq 1$ ordered elements:

$$\rho : \{1, 2, \dots n\} \to \{1, 2, \dots n\},$$

where $\rho(i) = k \in \{1, 2, \dots n\}$ and $i \neq j \implies \rho(i) \neq \rho(j)$. The product in S_n is the composition of permutations. The neutral element is the trivial permutation. The inverse element for such that $\rho(i) = k$ is $\rho^{-1}(k) = i$ for all $i, k \in \{1, \dots n\}$. The group is denoted S_n. We have $|S_n| = n!$, the number of all permutations of n elements.

Definition 7.4. Let $\sigma \in S_n$ be a permutation and consider the subgroup $\langle\sigma\rangle \subset S_n$ generated by σ. If the action of $\langle\sigma\rangle$ by permutations of the set of n elements contains exactly one nontrivial orbit with $k > 1$ elements (and possibly some fixed points), then $\sigma \in S_n$ is called a *k-cycle*.

Example 7.5. Let σ be the permutation in $S_{n\geq 6}$ that sends $1 \to 6$, $6 \to 3$ and $3 \to 1$. Then the subgroup generated by σ is cyclic of order 3: $\langle\sigma\rangle = \{1, \sigma, \sigma^2\}$, where 1 is the trivial permutation, σ sends $1 \to 6 \to 3 \to 1$, and σ^2 sends $1 \to 3 \to 6 \to 1$, and leaves the other elements fixed. Note that σ^3 sends $1 \to 1$, $3 \to 3$, and $6 \to 6$, so it is the trivial permutation. Then $\langle\sigma\rangle$ has one orbit with 3 elements and a few 1-element orbits. Therefore, σ is a 3-cylce.

Definition 7.6. A 2-cycle is called a *transposition*.

Notation 7.7. Let $\pi \in S_n$ be a k-cycle, and $x \in \{1, 2, \dots n\}$ a number in the nontrivial orbit of π. Then in the *cycle notation* we represent π as follows: $\pi = (x, \pi(x), \pi^2(x), \dots \pi^{k-1}(x))$.

Caution: Note that there are k choices for the starting element x in the cycle notation. In particular, the notations (123), (312) and (231) represent the same 3-cycle in $S_{n\geq 3}$. It sends $1 \to 2$, $2 \to 3$ and $3 \to 1$.

Example 7.8. In Example 7.5 the cycle $\sigma = (163)$ in the cycle notation.

Definition 7.9. Two cycles $\pi_1, \pi_2 \in S_n$ are *disjoint* if their nontrivial orbits do not intersect.

Example 7.10. The cycles (145) and (26) in S_6 are disjoint. The orbit of the first cycle is $\{1, 4, 5\}$ and the orbit of the second is $\{2, 6\}$. The cycles (531) and (254) in S_5 are not disjoint. Their orbits intersect: $\{1, 3, 5\} \cap \{2, 4, 5\} = \{5\}$.

Proposition 7.11. *Disjoint cycles commute in S_n.*

Proof: Let O_1 and O_2 be the nontrivial orbits of the cycles $p_1, p_2 \in S_n$, respectively. We assume that $O_1 \cap O_2 = \emptyset$. We will prove that $p_1p_2(x) = p_2p_1(x)$ for any $x \in \{1, 2, \dots n\}$. If $x \notin O_1 \cup O_2$, then $p_1(x) = x$ and $p_2(x) = x$, so that $p_1p_2(x) = x = p_2p_1(x)$. Now suppose that $x \in O_1$. This implies that $x \notin O_2$. Then we have:

$$p_1p_2(x) = p_1(x) = y; \qquad p_2p_1(x) = p_2(y) = y,$$

the last equality holds because $y = p_1(x) \in O_1$ and therefore $y \notin O_2$. The proof for $x \in O_2$ is similar.

Theorem 7.12. *Any permutation in S_n is a product of disjoint cycles, uniquely up to the order of the factors.*

Let $\sigma \in S_n$ and consider the cyclic subgroup $\langle\sigma\rangle \subset S_n$ generated by σ. Let $O_1, \dots O_k$ be the non-trivial orbits of the action of $\langle\sigma\rangle$ in the set $E = \{1, 2, \dots n\}$. Set $\pi_i = \sigma|_{X_i}$, $\pi_i = 1|_{E\setminus X_i}$. Then $\sigma = \pi_1\pi_2 \dots \pi_k$ by construction, where $\{\pi\}_{i=1}^k$ are disjoint cycles by construction. The presentation is unique up to the order of the cycles, because the disjoint cycles in any other presentation of σ will have to act in the same list of orbits $\{O_1 \dots O_k\}$, and the action in each orbit should coincide with that of σ.

Example 7.13. Computations with cycles. By Theorem 7.12 any element can be written as a product of disjoint cycles. Let us consider the permutation (1352)(256). The cycles are not disjoint, but we can rewrite this element as a product of disjoint cycles. Start with any number, for example 1: (1..... Consider the factors from right to left. The right factor does not move 1, and the left factor replaces it with 3: (13.... Go again from right to left, now tracking the number 3. It is sent to 5: (135.... Next, moving from right to left, track the number 5. It is sent to 6 by the right factor, and 6 is stabilized by the left factor, so we write (1356.... Next, 6 gets sent to 2 by the right factor and 2 to 1 by the left factor, therefore 6 is sent to 1, and we complete the cycle: (1356). Starting from any of the remaining numbers, we see that the permutation stabilizes 2 and 4. So we have: (1352)(256) = (1356).

It is easier to compute a conjugation $\pi\rho\pi^{-1}$ then a product of permutations in S_n.

Proposition 7.14. *Let $\pi, \rho \in S_n$. The cycle decomposition of $\pi\rho\pi^{-1}$ is obtained from that of ρ by replacing each integer i in the disjoint cycle decomposition of ρ by the integer $\pi(i)$.*

Proof: Let $E = \{1, 2, \dots n\}$. Recall that $\pi : E \to E$ is a bijection, and compute the action of $\pi\rho\pi^{-1}$ on and element $\pi(i)$. We have $\pi\rho\pi^{-1}(\pi(i)) = \pi(\rho(i))$. So whenever $\rho : i \to \rho(i)$, we have $\pi\rho\pi^{-1} : \pi(i) \to \rho(\pi(i))$. This means that replacing each i in the cycle notation for ρ by $\pi(i)$ gives a cycle notation for $\pi\rho\pi^{-1}$.

Example 7.15. For a 2-cycle, we have $(ij)^{-1} = (ij)$. Then (12)(13)(12) = (23) by Proposition 7.14. Also, (32)(1352)(32) = (1253), and $(265)(1352)(265)^{-1} = (265)(1352)(256) = (1326)$. (Check that (256)(265) = 1).

Proposition 7.16. *Every k-cycle in S_n is a product of $(k-1)$ transpositions. In particular,*

$$(12 \dots k) = (1k)(1\ \ k-1) \dots (13)(12).$$

Proof: Exercise (by induction on k).

Caution: The decomposition of a permutation as a product of *disjoint cycles* is unique. The transpositions in the Proposition above are *not* disjoint.

Corollary 7.17. *The group S_n is generated by the transpositions $\{(ij)\}_{1\le i<j\le n}$*

Proof: Any element $\sigma \in S_n$ is a product of disjoint cycles by Theorem 7.12. By Proposition 7.16 each cycle is a product of transpositions (not uniquely). Then each element $\sigma \in S_n$ is a product of transpositions.

Proposition 7.18. *No permutation in S_n can be written both as a product of an odd number of transpositions and as a product of an even number of transpositions.*

Idea of a proof: Consider the action of S_n by permutation of variables on the polynomial $\Delta_n = \prod_{1\le i<j\le n}(x_i - x_j)$. Then for any $\sigma \in S_n$, we have $\sigma(\Delta_n) = \pm\Delta(n)$. Set $\mathrm{sgn}(\sigma) = \pm 1$ accordingly. We have for $\tau, \sigma \in S_n$, that $\frac{\sigma\tau(\Delta_n)}{\Delta_n} = \frac{\sigma(\Delta_n)}{(\Delta_n)} \cdot \frac{\sigma\tau(\Delta_n)}{\sigma(\Delta_n)}$. It follows that the map $S_n \to \pm 1$ that sends $\sigma \to \mathrm{sgn}(\sigma)$ is a group homomorphism. It is also clear that $\mathrm{sgn}(12) = -1$, as there is only one change of sign in Δ_n: $(x_1 - x_2) \to (x_2 - x_1)$. Now for any i, k we can write $(1k) = (2k)(12)(2k)^{-1}$ and $(ik) = (1i)((1k)(1i)^{-1}$. Then using the homomorphism property one can show that $\mathrm{sgn}(ik) = -1$ for any transposition $(ik) \in S_n$.

The previous proposition allows us to define the sign of a permutation as follows.

Definition 7.19. A permutation is *odd* if it is a product of an odd number of transpositions, and *even* if it is a product of an even number of transpositions. A transposition is an odd permutation.

Proposition 7.20. *The set A_n of all even permutations form a normal subgroup in S_n of index 2: $[S_n : A_n] = 2$.*

Proof: The map $\Phi : S_n \to \{\pm 1\}$ sending $\sigma \to \mathrm{sgn}(\sigma)$, is a group homomorphism. Its kernel is a normal subgroup of S_n that consists exactly of the even permutations in S_n. Since $\mathrm{im}(\Phi) \simeq S_n/\ker(\Phi)$, we have $[S_n : \ker(\Phi)] = |\mathrm{im}(\Phi)| = 2$, and by definition $A_n = \ker(\Phi)$.

Definition 7.21. The group A_n is called the *alternating group* of n elements.

Example 7.22. Let us write the elements of the symmetric group S_3 in the cycle notation:

$$S_3 = \{1, (12), (13), (23), (123), (132)\}.$$

The alternating group $A_n = \{1, (123) = (13)(12), (132) = (12)(13)\}$. In this case the alternating group is isomorphic to the cyclic group C_3.

Definition 7.23. A nontrivial group G is called simple if it does not contain a *normal* subgroup except $\{1\}$ and itself.

Theorem 7.24. *The alternating group A_n is simple for $n \ge 5$.*

For a proof see the file "Symmetric group" in Resources (in French).

8 The orbit-stabilizer theorem.

Let G be a finite group acting on a finite set E. Then the orbit of $x \in E$ is the set $\mathrm{Orb}_x = \{g \cdot x \in G\}$ (see Definitions 7.1 7.2).

Definition 8.1. Let G act on the set E. The *stabilizer* of $x \in E$ is

$$\mathrm{Stab}_x = \{g \in G \,|g \cdot x = x\}.$$

Proposition 8.2. *Let G act on the set E. The stabilizer Stab_x of an element $x \in E$ is a subgroup in G.*

Proposition 8.3. *Let G act on the set E. Two orbits of the G-action Orb_x and Orb_y either coincide, or do not intersect. In particular, E splits as a disjoint union of orbits of G-action: $E = \cup_i \mathrm{Orb}_{x_i}$.*

Proofs of Propositions 8.2 and 8.3: exercise. (If $g \cdot x = f \cdot y$, then $f^{-1}g \cdot x = y$ and $y \in \mathrm{Orb}_x$, therefore $G \cdot y = \mathrm{Orb}_y \subset \mathrm{Orb}_x$. Similarly $\mathrm{Orb}_x \subset \mathrm{Orb}_y$).

Example 8.4. Consider the action of the group $D_3 = \langle r, s \mid r^3 = 1, s^2 = 1, srs = r^{-1}\rangle$ on itself by conjugations. In this case $G = E = D_3$, and the action is given by $g \cdot x = gxg^{-1}$ for any $g \in D_3, x \in D_3$. Then $\{1\}$ is the fixed point of the action: $g1g^{-1} = 1$ for all $g \in D_3$. The elements $\{r, r^2\}$ form another orbit: $srs^{-1} = srs = r^{-1} = r^2$, and all rotations commute. Finally, the remaining elements form a single orbit: $\{s, sr, sr^2\}$ because $rsr^{-1} = sr^{-2} = sr$, $r^2sr^{-2} = r^{-1}sr = sr^2$. We have: $\mathrm{Orb}_1 = \{1\}$, $\mathrm{Orb}_r = \{r, r^2\}$, $\mathrm{Orb}_s = \{s, sr, sr^2\}$. The stabilizer of 1 is the whole group, and the stabilizer of r and r^2 is the subgroup of rotations $\mathrm{Stab}_r = \mathrm{Stab}_{r^2} = \langle r\rangle \subset D_3$. The stabilizer of s is the subgroup $\mathrm{Stab}_s = \langle s\rangle \subset D_3$, since sr or sr^2 do not stabilize it: $srs(sr)^{-1} = srsr^{-1}s = sr^2$, nor do the rotations. Similarly, the stabilizer of sr is the subgroup $\mathrm{Stab}_{sr} = \langle sr\rangle \subset D_3$, and the stabilizer of sr^2 is the subgroup $\mathrm{Stab}_{sr^2} = \langle sr^2\rangle \subset D_3$.

Theorem 8.5. *(The Ortbit-Stabilizer theorem). Let a finite group G act on a finite set E. Then for any element $x \in E$, the number of elements in the orbit of x under the G-action equals to the index of the stabilizer subgroup of x in G:*

$$|\mathrm{Orb}_x| = [G : \mathrm{Stab}_x].$$

Proof: Let $H = \mathrm{Stab}_x \subset G$ and consider the left H-cosets in G. There is a bijection between the set $\{gH\}_{g\in G}$ of left H-cosets in G and the elements of x-orbit Orb_x. Namely,

$$\mu : gH \to g \cdot x$$

is a bijection between $\{gH\}_{g\in G}$ and Orb_x. Indeed, μ is surjective because any element of G belongs to a left H-coset. The map μ is also injective because if $\mu(gH) = \mu(fH)$ for some $g \neq f$ in G, then $g \cdot x = f \cdot x$, therefore $f^{-1}g \cdot x = x$, then $f^{-1}g \in \mathrm{Stab}_x = H$, and therefore $gH = fH$. We conclude that μ is a bijection, which implies that the number of elements in both sets coincide: $|\mathrm{Orb}_x| = [G : \mathrm{Stab}_x]$.

Example 8.6. Let us use the Orbit-Stabilizer theorem to find the order of the group G of rotational symmetries of a cube. Consider the action of G on the set of all faces of the cube. Let f be one of the faces. Then $\mathrm{Stab}_f \subset G$ contains the rotations stabilizing f and the opposite face, and is isomorphic to the cyclic group of order 4. The orbit of f consists of all faces of the cube and has order 6. Therefore,

$$|\mathrm{Orb}_f| = [G : \mathrm{Stab}_f] = |G|/|\mathrm{Stab}_f| \quad \Longrightarrow \quad 6 = |G|/4 \quad \Longrightarrow \quad |G| = 24.$$

The group of rotational symmetries of a cube has order 24.
One can obtain the same result by considering the action of G on the set of vertices or edges of the cube.

9 Conjugacy classes and the class equation

Definition 9.1. Let G be a group acting on itself by conjugations: $g \cdot x = gxg^{-1}\ \forall x \in G, g \in G$. Then an orbit of $x \in G$ is called the *conjugacy class* of x in G and denoted C_x, and the stabilizer of x with respect to this action is called the *centralizer* of $x \in G$ and denoted $G_x \subset G$.

Example 9.2. In the example 8.4 we have $C_r = \{r, r^2\}$, and $G_r = \langle r\rangle$, the subgroup of rotations in D_3. Also, $C_s = \{s, sr, sr^2\}$ and $G_s = \langle s\rangle$, a subgroup in D_3.

Proposition 9.3. *The elements $g_1 \in S_n$ and $g_2 \in S_n$ belong to the same conjugacy class in S_n if and only if they decompose as a product of disjoint cycles of the same lengths. The set of lengths of cycles in a disjoint cycle decomposition of an element $g \in S_n$ is called the cycle type of g. Conjugacy classes in S_n are in bijection with cycles types.*

Proof: PS6, Ex. 2.

Definition 9.4. The *center* $Z(G)$ of the group G is the set of elements that commute with any element in G:

$$Z(G) = \{x \in G \mid xg = gx\ \forall g \in G\}.$$

Remark 9.5. Let $x \in G$. Then x is in the center if and only if the centralizer of x is the whole group G, and the conjugacy class of x contains a single element:

$$x \in Z(G) \quad \Leftrightarrow \quad G_x = G, \ \ C_x = \{x\}.$$

Indeed, $gx = xg\ \forall g \in G$ is equivalent to $gxg^{-1} = x$ for all $g \in G$.

Theorem 9.6. *(The class equation). Let G be a finite group, and let $Z(G)$ be its center, and $\{x_i\}_{i=1}^m$ a set of representatives the conjugacy classes $\{C_{x_i}\}_{i=1}^m$ containing more than one element each. Let G_{x_i} be the stabilizer subgroup for x_i. Then*

$$|G| = |Z(G)| + \sum_{i=1}^{m} |C_{x_i}| = |Z(G)| + \sum_{i=1}^{m} [G : G_{x_i}].$$

Proof: The first formula is a direct consequence of Proposition 8.3. Indeed, under the adjoint action of G we have $|G| = \sum_{j=1}^{r} |C_j|$, where $\{C_j\}_{j=1}^r$ are all the conjugacy classes in G. By definition, the center of G is the union of all one-element conjugacy classes, $Z(G) = \cup_{k=1}^{t} C_k$. Then $|G| = |Z(G)| + \sum_{i=1}^{m} |C_{x_i}|$, where $\{C_{x_i}\}_{i=1}^m$ are all the nontrivial conjugacy classes. The second formula follows from the Orbit-Stabilizer theorem Theorem 8.5.

Example 9.7. We can use the class equation to show that any group of order p^n, where p is a prime and n a positive integer, has a nontrivial center. First, the class equation $|G| = p^n = |Z(G)| + \sum_i [G : G_{x_i}]$ means that $|Z(G)|$ is a multiple of p, since the numbers $|G|$ and $[G : G_{x_i}]$ are multiples of p. Also, $Z(G) \ni 1$ and so $|Z(G)| \geq 1$. Therefore, $Z(G)$ contains at least p elements.

10 Direct product of groups

Definition 10.1. Let G, H be groups. The *direct product* $G \times H$ is the group whose elements are pairs $G \times H = \{(g, h) \mid g \in G, h \in H\}$ with the multiplication $(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2)$ for any $g_1, g_2 \in G, H_1, h_2 \in H$.

It is easy to check that $(1_G, 1_H) \in G \times H$ is the identity element, and $(g, h)^{-1} = (g^{-1}, h^{-1})$.

Proposition 10.2. *Properties of the direct product:*

(a) $G \times H \simeq H \times G$

(b) $G \times H$ *is abelian if an only if* G *and* H *are both abelian*

(c) $\{(1, h\}_{h \in H} \subset G \times H$ *is a subgroup isomorphic to* H*, and* $\{(g, 1\}_{g \in G} \subset G \times H$ *is a subgroup isomorphic to* G

(d) For the cyclic groups, $C_n \times C_m \simeq C_{mn}$ *if and only If* $\gcd(n, m) = 1$

(e) Suppose that $H, K \subset G$ *are two subgroups such that (a)* $H \cap K = \{1\}$*, (b)* $\forall h \in H, k \in K$*,* $hk = kh$*, (c)* G *is spanned by the products* $\{hk\}_{h \in H, k \in K}$*. Then* $G \simeq H \times K$*.*

Proof:

(a) The map $\phi : G \times H \to H \times G$ exchanging the order of factors is an isomorphism of groups.

(b) If $G \times H$ is abelian, then in particular $(1, h_1)(1, h_2) = (1, h_2)(1, h_1)$ for any $h_1, h_2 \in H$, so that H is necessarily abelian.

(c) The map $\psi_1 : G \to G \times H$ defined as $\psi_1(g) = (g, 1)$ and the map $\psi_2 : H \to G \times H$ defined as $\psi_2(h) = (1 \times h)$ are clearly injective group homomorphisms.

(d) Let t and q be elements of C_n and C_m respectively. Then the order of (t, q) in $C_n \times C_m$ is $\leq \mathrm{lcm}(n, m)$, with the equality achieved if t and q are generators of their respective groups. The number $\mathrm{lcm}(n, m)$ equals to mn if and only if $\gcd(m, n) = 1$.

(e) We will check that the map $\phi : H \times K \to G$, sending (h, k) to $hk \in G$, is a group isomorphism. We have $\phi(1, 1) = 1 \in G$, and $\phi((h_1, k_1))\phi((h_2, k_2)) = h_1 k_1 h_2 k_2 = h_1 h_2 k_1 k_2 = \phi((h_1, k_1), (h_2, k_2))$, where we used the property (b) of the conditions. Therefore, ϕ is a group homomorphism. The surjectivity of ϕ is assured by the property (c). If $\phi(h, k) = hk = 1$, then $k = h^{-1}$. Since by property (a) we have $H \cap K = \{1\}$, this implies $k = h^{-1} = 1$, and therefore $\phi : H \times K \to G$ is injective. This completes the proof.

11 Classification of finite abelian groups.

Definition 11.1. A group G is *simple* if it has no nontrivial ($\neq \{1\}$) proper ($\neq G$) normal subgroups.

Theorem 11.2. *(Cauchy). If G is a finite abelian group and a prime p divides the order of G, then G contains an element of order p.*

Proof: Assume G is the smallest counter-example for a given prime p. Consider $\langle g\rangle \subset G$, where $g \in G$ is a nontrivial element. By the assumption the order of g is not divisible by p. Then the quotient group $G/\langle g\rangle$ has the order divisible by p. Since G was the smallest counter-example, there exists an element of order p in $G/\langle g\rangle$, say $(h\langle g\rangle)^p = 1$, then $h^p \in \langle g\rangle$, and so there exists a power of h with order p.

Remark 11.3. In fact Cauchy's theorem states the same property for any finite group. See PS7 for a proof.

Corollary 11.4. *If G is a finite abelian simple group, then G is isomorphic to a cyclic group of prime order.*

Proof: Any subgroup is normal in an abelian group. If the order of G is divisible by p, then it contains a subgroup generated by an element of order p, which is a cyclic group of order p. Therefore the only abelian simple finite groups are cyclic groups of prime order.

To classify all finite abelian groups we will use direct products to build more complicated groups out of smaller groups.

Definition 11.5. Let n be a positive integer. A *partition* of n is a set of positive integers $i_1 \geq i_2 \geq \ldots \geq i_k \geq 1$ such that $i_1 + i_2 + \ldots + i_k = n$.

Example 11.6. There are 7 partitions of $n = 5$: $(5), (4,1), (3,2), (3,1,1), (2,2,1), (2,1,1,1), (1,1,1,1,1)$.

Proposition 11.7. *Let G be an abelian group of prime power order, $|G| = p^n$. Then G is isomorphic to a direct product of cyclic groups $G = C_{p^{i_1}} \times C_{p^{i_2}} \times \ldots \times C_{p^{i_k}}$, where $(i_1 \geq i_2 \geq \ldots i_k)$ is a partition of n. Different partitions of n correspond to non-isomorphic abelian groups.*

Idea of a proof: This is the hardest part of the classification result. Here are the steps of the proof:
(1) Let $g \in G$ be an element of highest order in G. We have $o(g) = p^k$ with $k \leq n$. Consider the quotient group $G/ < g >= \{x_1 < g >, x_2 < g >, \ldots x_t < g >\}$. Show that any conjugacy class $x < g >$ contains an element $y \in x < g >$ such that the order of y in G equals to the order of $x < g >$ in $G/ < g >$.
(2) Suppose we write $G/ < g > \simeq < y_1 < g >> \times ... \times < y_t < g >>$. Then prove that $G \simeq < g > \times < y_1 > \times ... \times < y_t >$. The isomorphism follows from comparing the orders of the groups using (1).
(3) Finally we derive that for $|G| = p^n$, there exists a subgroup $H \subset G$ such that $G \simeq < g > \times H$, where g is an element of maximal order p^k in G, and $|H| = p^{n-k}$. By induction, the statement of the proposition follows.
See the file "FiniteAbelianGroups" in the Resources for details.

Example 11.8. If G is an abelian group with $|G| = 8$, then G is isomorphic to one of the following groups:

$$C_8, \quad C_4 \times C_2, \quad C_2 \times C_2 \times C_2.$$

These groups are non-isomorphic because the last one contains only elements of order 2, the middle one contains also an element of order 4, and the first one is the only one that contains an element of order 8.

Proposition 11.9. *Let G be a finite abelian group, and $|G| = p_1^{n_1} \ldots p_r^{n_r}$ is the prime factorization of $|G|$ (here p_i are all distinct primes). Then G is isomorphic to a direct product of abelian groups of orders $p_1^{n_1}, p_2^{n_2}, \ldots p_r^{n_r}$:*

$$G \simeq G_{p_1^{n_1}} \times G_{p_2^{n_2}} \times \ldots G_{p_r^{n_r}}.$$

Proof: If $|G| = mn$, with $\gcd(m,n) = 1$, and $H = \{g \in G : o(g)|m\}$, $K = \{g \in G : o(g)|n\}$, then H and K are clearly subgroups of G. Moreover, one can check using Proposition 10.2 (e), that we have $G \simeq H \times K$. Indeed, $H \cap K = 1$ because if the order of an element divides both n and m, then it is 1 because $\gcd(n,m) = 1$. Let us prove that $G = \{hk\}_{h \imath H, k \in K}$. Let $g \in G$ be such that its order $o(g) = st$, where $s|m$ and $t|n$, so that $g \notin H$ and $g \notin K$. Then $g^s \in G$ has order t, and $g^t \in G$ has order s, therefore $g^s = k \in K$ and $g^t = h \in H$. We have $\gcd(s,t) = 1$, therefore by Bezout's theorem there exist $x, y \in \mathbb{Z}$ such that $xs + yt = 1$, and therefore $k^x h^y = g$, where $k^x \in K$ and $h^y \in H$. Then by Proposition 10.2 (e) we have $G \simeq H \times K$. By induction, the statement follows.

Theorem 11.10. *(Classification of finite abelian groups). Let G be a finite abelian group. Then G is isomorphic to a direct product of cyclic groups with prime power orders:*

$$G \simeq C_{p_1^{a_1}} \times C_{p_2^{a_2}} \times \ldots C_{p_m^{a_m}},$$

where $\{p_1, \ldots p_m\}$ are primes, not necessarily distinct, and $|G| = p_1^{a_1} p_2^{a_2} \ldots p_m^{a_m}$.

Proof: The classification theorem follows from Proposition 11.7 Proposition 11.9 .
An alternative proof, independent of the Proposition 11.7, can be given using the generators and relations presentation of a finite abelian group. Suppose $G = \langle g_1, g_2, \dots g_k | R_1, R_2, \dots R_l \rangle$, where g_i are the generators and R_j the relations that define the group G. The relations are of the form $R_j \ : \ g_1^{n_{i1}} g_2^{n_{i2}} \dots g_k^{n_{ik}} = 1$. The system of generators and relations can be written in the form of a rectangular matrix

$$\begin{pmatrix} n_{11} & n_{12} & \dots & n_{1k} \\ n_{21} & n_{22} & \dots & \\ \dots & \dots & & \\ n_{l1} & n_{l2} & \dots & n_{lk} \end{pmatrix}$$

We can see that the usual row-column operations with integer coefficients leave the group unchanged:

1. Swapping two rows corresponds to changing the order of relations; swapping two columns corresponds to changing the order of generators.
2. Adding an integer multiple of one row to another row corresponds to multiplying one relation by an integer power of another relation, which leads to the same group. Example: $G = \langle g, h | g^3 h = 1, gh^{-2} = 1 \rangle$ is equivalent to $G = \langle g, h | g^5 h^{-3} = 1, gh^{-2} = 1 \rangle$, where we have multiplied $g^3 h = 1$ by the square of $gh^{-2} = 1$. This corresponds to the matrix transformation
$$\begin{pmatrix} 3 & 1 \\ 1 & -2 \end{pmatrix} \longrightarrow \begin{pmatrix} 5 & -3 \\ 1 & -2 \end{pmatrix}.$$
3. Adding an integer multiple of a column to another column corresponds to redefining the set of generators by passing from one generator to a product of it with a power of another generator, which leads to the same group. Example: $G = \langle g, h | g^n h^m = 1 \rangle$ is equivalent to $G = \langle t, h | t^n h^{m+3n} = 1 \rangle$, where $t = gh^{-3}$. Indeed, $(gh^{-3})^n h^{m+3n} = g^n h^{-3n} h^{m+3n} = g^n h^m = 1$, so that the group defined in terms of $\{h, g\}$ with the relation $g^n h^m = 1$ is isomorphic to the group defined by t, h with the relation $t^n h^{m+3n} = 1$ by the isomorphism sending $g \to t$ and $h \to h$. This operation corresponds to the matrix transformation
$$\begin{pmatrix} n & m \end{pmatrix} \longrightarrow \begin{pmatrix} n & m + 3n \end{pmatrix}.$$

Applying the row and column operations, we can get n_{11} to be the smallest possible by absolute value, which is the gcd of the elements of the first row and the first column. Therefore, the new n_{11} divides all elements in the first row and the first column. Applying the row and column operations with integer coefficients further, we can obtain the matrix of the form

$$\begin{pmatrix} n_{11} & 0 & \dots & 0 \\ 0 & n_{22} & \dots & \\ \dots & \dots & & \\ 0 & n_{l2} & \dots & n_{lk} \end{pmatrix}$$

We can continue repeating the operation with the smaller matrix starting from the second column and row, and eventually obtain a diagonal matrix of size $r = \min(k, l)$

$$\begin{pmatrix} n_{11} & 0 & \dots & 0 \\ 0 & n_{22} & \dots & 0 \\ \dots & \dots & & \\ 0 & 0 & \dots & n_{rr} \end{pmatrix}.$$

This matrix defines a group isomorphic to the original group G. On the other hand, it is given in generators and relations as follows: $G = \langle g_1, \dots g_k | g_1^{n_{11}} = 1, \dots g_r^{n_{rr}} = 1 \rangle$. Denote $G_i = \langle g_i | g_i^{n_{ii}} = 1 \simeq C_{n_{ii}}$. This is a cyclic group and a subgroup in G. We have $G_i \cap G_j = \{1\}$, and $g_i g_j = g_j g_i$ since the group G is abelian. The powers of $\{g_i\}_{i=1}^r$ generate G. Therefore, by the properties of the direct product of groups, $G \simeq C_{n_{11}} \times C_{n_{22}} \times \dots \times C_{n_{rr}}$, a direct product of cyclic groups. Each cyclic group $C_{n_{ii}}$ is in turn a direct product of cyclic groups of prime power orders according to the prime factorization of n_{ii}, which follows from the property (d) of Proposition 10.2. Finally, $G \simeq C_{p_1^{a_1}} \times C_{p_2^{a_2}} \times \dots \times C_{p_m^{a_m}}$ is a direct product of cyclic groups of prime power orders. This completes the proof.

Definition 11.11. The numbers $(p_1^{a_1}, p_2^{a_2}, \dots, p_m^{a_m})$ are called the *elementary divisors* of G.

Theorem 11.12. *Let G be a finite abelian group. Then G is isomorphic to a direct product of cyclic groups with consecutively dividing orders:*

$$G \simeq C_{d_1} \times C_{d_2} \times \dots C_{d_k},$$

where $d_k | d_{k-1}$, $d_{k-1} | d_{k-2}$ and so on, $d_2 | d_1$, and $|G| = d_1 d_2 \dots d_k$.

This follows from Theorem 11.10 and the property of direct products of cyclic subgroups of mutually prime orders. Indeed, $C_{p^t} \times C_{q^s} = C_{p^t q^s}$, if p and q are distinct primes. Taking the direct product of the highest powers of each distinct prime in the decomposition of Theorem 11.10, we can form the largest cyclic group C_{d_1}. Then we take the highest powers of the remaining distinct primes, and so on.

Definition 11.13. The numbers $(d_k, d_{k-1}, \dots d_2, d_1)$ are called the *invariant factors* of G.

Example 11.14. Let G be an abelian group, $|G| = 360 = 2^3 \cdot 3^2 \cdot 5$. The partitions of the power of 2 are $(3), (2,1), (1,1,1)$. The partitions of the power of 3 are $(2), (1,1)$. According to Theorem 11.10, we have the following list of unisomorphic abelian groups of order 360:

$$C_8 \times C_9 \times C_5, \quad C_8 \times C_3 \times C_3 \times C_5, \quad C_4 \times C_2 \times C_9 \times C_5, \quad C_4 \times C_2 \times C_3 \times C_3 \times C_5,$$

$$C_2 \times C_2 \times C_2 \times C_9 \times C_5, \quad C_2 \times C_2 \times C_2 \times C_3 \times C_3 \times C_5.$$

The elementary divisors are $(8,9,5), (8,3,3,5), (4,2,9,5), (4,2,3,3,5), (2,2,2,9,5), (2,2,2,3,3,5)$. Let us collect the powers of distinct primes to rewrite the same list of groups according to Theorem 11.12:

$$C_{360}, \quad C_{120} \times C_3, \quad C_{180} \times C_2, \quad C_{60} \times C_6, \quad C_{90} \times C_2 \times C_2, \quad C_{30} \times C_6 \times C_2.$$

The invariant factors of G are $(360), (120,3), (180,2), (60,6), (90,2,2), (30,6,2)$.

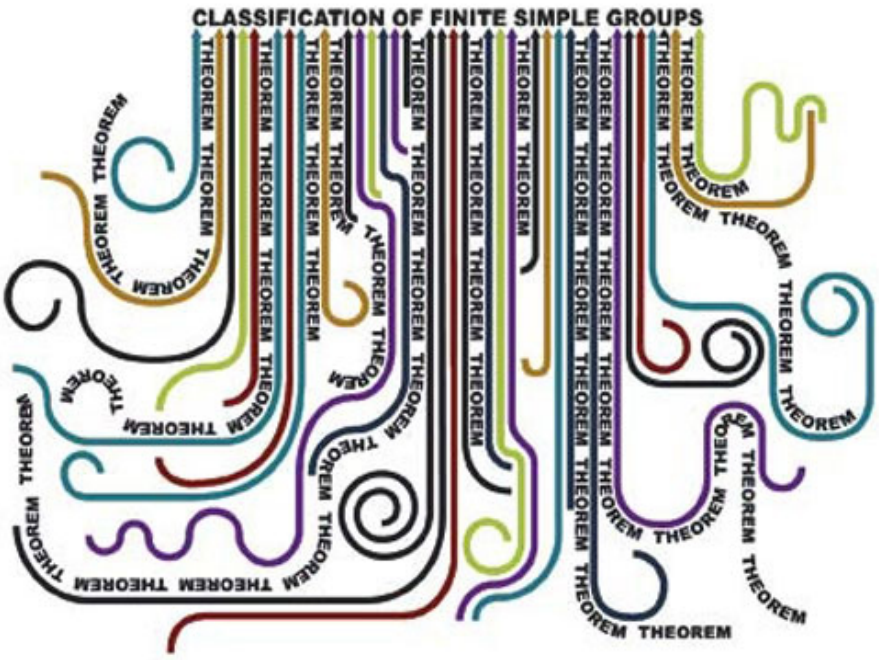
The contents of the Appendices is not included in the exam.

12 Appendix A: Classification of finite simple groups.

Recall that Theorem 11.4 provides a classification of all finite simple abelian groups: these are cyclic groups of prime order. A much harder question is the classification of all finite simple groups. We will outline the answer below.

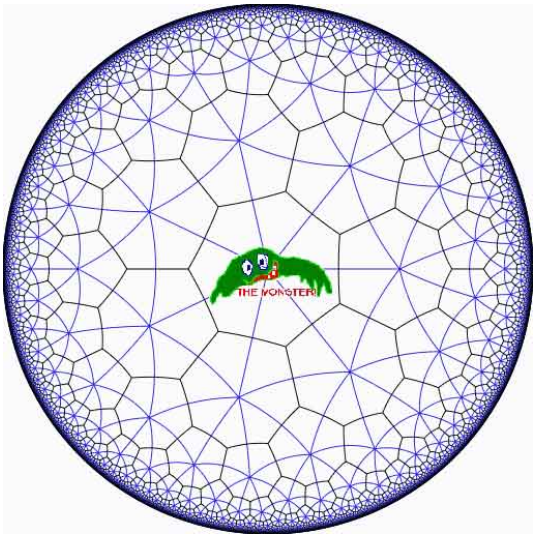
Recall that by Theorem 7.24 we have: for $n > 5$ the alternating group A_n is simple. The proof is relatively easy and is based on the elementary properties of the symmetric group. See the file "Symmetric group" in Resources.

So we already know two families of simple groups: $\{C_p\}_{p \text{ prime}}$ and $\{A_n\}_{n\geq 5}$. The rest of the classification is much harder to prove. The complete argument includes hundreds of theorems proven by mathematicians over the last hundred and eighty years and contains thousands of pages of text. Here is one specialist's vision of the complexity of the classification argument.



Theorem 12.1. *(Gorenstein, Aschbacher, Lyons, Smith, and more than 30 other authors, 1832-2012) Let G be a finite simple group. Then G is one of the following:*

1. *A cyclic group C_p, p a prime*
2. *An alternating group A_n for $n \geq 5$*
3. *A group of Lie type. They form 16 infinite families of groups similar to matrix groups with coefficients taken to be integers modulo a prime. (For example, the 2×2 matrices with entries in $\mathbb{Z}/5\mathbb{Z}$ and determinant equal to $[1]_5$ form a simple group. But this group turns out to be isomorphic to the alternating group A_5, already listed above. However, examples of this kind provide infinitely many new simple finite groups).*
4. *One of the 26 sporadic groups, or the Tits group. These are the remaining 27 exceptional groups. The sporadic groups often appear as groups of automorphisms of lattices in higher dimensional spaces. For example, the Conway sporadic group Co_1 is the group of automorphisms of a remarkable lattice in R^{24}. The vertices of this lattice provide the arrangement of 196560 unit balls in $\mathbb{R}^{24}$, all touching the same central unit ball. This is the largest possible number of unit balls touching the same central unit ball in R^{24}. (For comparison, the maximal number of unit balls touching the same central unit ball in R^2 is 6, and the corresponding arrangement is given, as you might have guessed, by the hexagonal lattice). The order of the group Co_1 is about $4 \cdot 10^{18}$. The largest simple finite sporadic group is the Monster. Its order is about $8 \cdot 10^{53}$. It also arises as a group of automorphisms of a lattice. The image below is a picture, in some sense, of the Monster.*



The Monster

13 Appendix B: Examples of groups we didn't have time to consider.

Example 13.1. The braid group B_n on n strings, $n \geq 2$.

- Elements: n strings hanging between two horizontal axes attached at the top and the bottom at equal intervals, possibly tangled in the middle.
- Multiplication: the tangle ab is obtained by attaching the top of the tangle b to the bottom of the tangle a and removing the horizontal axes in the middle.
- Identity element: n parallel vertical strings
- The inverse tangle for a tangle a is designed to untangle every crossing in a starting from the bottom up, to obtain n parallel vertical srtings.

The group B_n is infinite and non-abelian.

Example 13.2. The fundamental group of a topological space $\pi_1(M)$.

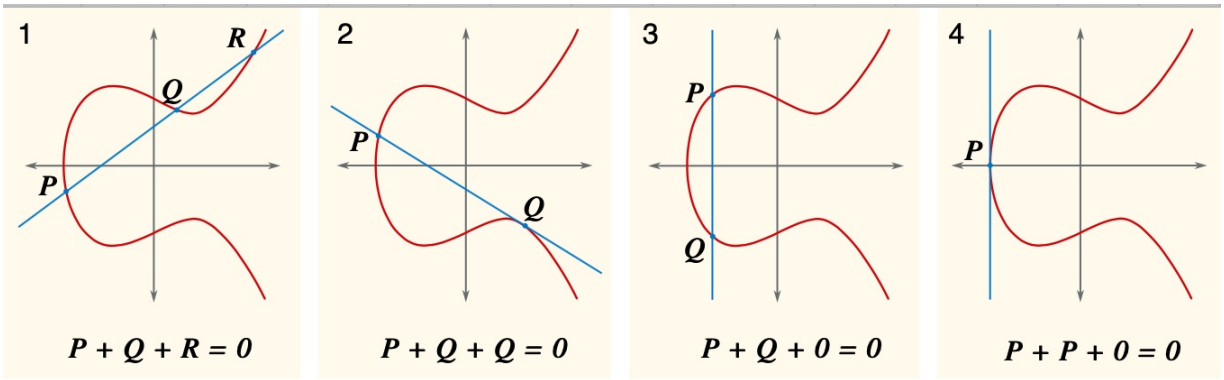
- Elements: Directed loops in M starting and ending at a fixed point in M, up to stretching and pulling
- Multiplication: Concatenation of loops
- Identity element: The loop of zero length
- The inverse loop a^{-1} is the loop a traced in the opposite direction

The properties of the group $\pi_1(M)$ depend on the properties of the topological space M.

Example 13.3. The abelian group of an elliptic curve $y^2 = x^3 + ax + b$.

- Elements: points on the curve in the projective plane (with an additional point at infinity O).
- Multiplication: draw a line through two points P and Q. Then $P + Q$ is the opposite point, symmetric with respect to the x-axis of the third point of intersection of the line with the curve (see the picture below). The proof of the associativity of multiplication requires some work.
- Identity element: The point at infinity O.
- The inverse element to P is the opposite point $-P$, symmetric with respect to the x-axis.

This is an infinite abelian group.



Example 13.4. The Rubik's cube group G_{RC}

- Elements: Rubik's cube moves
- Multiplication: Composition of moves
- Identity element: The empty move
- The inverse element: The move that returns the cube to its initial state

The group G_{RC} is a finite non-abelian group of order $2^{27} \cdot 3^{14} \cdot 5^3 \cdot 7^2 \cdot 11$. For more details on the Rubik's cube group, see "Group Theory and the Rubik's Cube.pdf" in Resources.

Example 13.5. Conway's group of two-player games

- Elements: Two-player games without an element of chance, where there is always a looser - a player who has no available moves.
- Multiplication: Placing two games side by side and allowing each player to take a move in any one of the games
- Identity element: Any game where the player who starts *second* can force a win. For example, an empty game (the first player has to move first, so he loses).
- The inverse element: The game g^{-1} is the game g where all the moves of the left player are available to the right player, and vice versa. Then if g and g^{-1} are placed side by side, the second player can force a win by reproducing the moves of the first player. The first player runs out of moves first.

This is an infinite abelian group. The best reference on this group is the book "Winning Ways for Your Mathematical Plays" by Elwyn R. Berlekamp, John H. Conway and Richard K. Guy.