GROUP THEORY: LECTURE NOTES 2018

DMITRI ZAITSEV

Abstract. These are very sketchy notes only aimed to supplement the other literature

Contents

1. Sets

The set S is defined when for every element a it is known whether a belongs to S, written $a \in S$. S is a *subset* of T if for every $x \in S$, one has $x \in T$. If $S \subset T$ and $T \subset R$, then $S \subset R$.

1.1. **Set operations.** For sets A, B (usually subsets in a larger set) the *union* $A \cup B$, *intersection* $A \cap B$, and *difference* $A \setminus B$ are defined by

$$A \cup B = \{x : a \in A \text{ or } a \in B\},$$
$$A \cap B = \{x : a \in A \text{ and } a \in B\},$$
$$A \setminus B = \{x : a \in A \text{ and } a \notin B\}.$$

They satisfy the following basic relations:

$$(A \cap B) \cap C = A \cap (B \cap C), \quad (A \cup B) \cup C = A \cup (B \cup C),$$
$$(A \cap B) \cup C = (A \cup C) \cap (B \cup C), \quad (A \cup B) \cap C = (A \cap C) \cup (B \cap C),$$
$$(A \cap B) \setminus C = (A \setminus C) \cap (B \setminus C), \quad (A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C),$$
$$A \setminus (B \cup C) = (A \cup C) \setminus (B \cup C), \quad (A \cap C) \setminus B = (A \cap C) \setminus (B \cap C).$$

Also consider the *Cartesian product* $A \times B$, which is the set of all ordered pairs (a, b) with $a \in A$, $b \in B$.

1.2. **Basic number sets.** *Natural numbers* $\mathbb{N}$ (which we assume to contain 0 as a matter of convention), *integers* $\mathbb{Z}$, *rational numbers* $\mathbb{Q}$, *real numbers* $\mathbb{R}$, *complex numbers* $\mathbb{C}$, *quaternions* $\mathbb{H}$.

2. Maps

Maps or *mappings* are defined between two sets S and T:

$$f\colon S \to T,$$

where S is the *domain* or *source* and T is the *codomain* or *target* of f. For any subsets $A \subset S, B \subset T$ we have the *image*

$$f(A) := \{f(x) : x \in A\}$$

and the *preimage*

$$f^{-1}(B) := \{x \in S : f(x) \in B\}.$$

Definition 2.1. A map $f\colon S \to T$ is *injective* if $f(x) = f(x')$ implies $x = x'$ for any $x, x' \in S$. A map $f\colon S \to T$ is *surjective* if for every $y \in T$ there exists $x \in S$ with $f(x) = y$, or, equivalently $f(S) = T$. The map f is *bijective* whenever it is both injective and surjective.

2.1. **Compostion of maps.** For maps $f\colon S \to T$ and $g\colon T \to R$ their *composition* $g \circ f$ is defined by

$$(g \circ f)(x) = g(f(x)).$$

Definition 2.2. The *inverse* of $f\colon S \to T$ is any map $f^{-1}\colon T \to S$ satisfying (1) and (2), where

(1) $f^{-1}(f(x)) = x$ for all $x \in S$ (equivalently $f^{-1} \circ f = \mathsf{id}_S$);
(2) $f(f^{-1}(y)) = y$ for all $y \in T$ (equivalently $f \circ f^{-1} = \mathsf{id}_T$).

If (1) holds, f^{-1} is called a *left inverse*, if (2) holds, it is called a *right inverse*.

It inverse exists, it is necessarily unique (special case of the uniqueness of the inverse for abstract groups). Note that right and left inverses are not unique in general.

Example 2.3. The map $f\colon \{0\} \to \{0, 1\}$, $f(0) = 0$, is the simplest example of a map with left but not right inverse. The map $f\colon \{0, 1\} \to \{0\}$, $f(0) = f(1) = 0$, is the simplest example of a map with right but not left inverse.

Proposition 2.4. *A map $f\colon S \to T$ has inverse if and only if it is bijective.*

3. Binary operations

A *binary operation* on a set S is any map $*\colon S \times S \to S$, $(a, b) \mapsto a * b$. A binary operation may or may not be *associative* and *commutative*.

Composition of maps is always associative but not commutative in general. Note that composition is a binary operation in the special case of composing self-maps of a given set but associativity

$$(h \circ g) \circ f = h \circ (g \circ f)$$

holds in full generality, i.e for any triple of maps

$$f\colon A \to B, \quad g\colon B \to C, \quad h\colon C \to D.$$

4. Groups

A *group* is a set G with binary operation $*$ such that

(A1) $*$ is associative;
(A2) there exists an identity (or unit) element e with $e * x = x * e = x$ for every $x \in G$;
(A3) every $x \in G$ has inverse x^{-1} such that $x^{-1} * x = x * x^{-1} = e$.

Both identity and unit terminologies are used for e. However, one has to be careful not to confuse e with a unit in ring (any invertible element under multiplication), and not to confuse e with the identity map of the set into itself.

In a group every element b can be divided by another element a on the right or on the left:

Lemma 4.1. *If G is a group, for every $a, b \in G$, the equations*

$$ax = b, \quad ya = b$$

have the unique solutions $x = a^{-1}b$, $y = ba^{-1}$ respectively.

Definition 4.2 (Semi-groups and monoids)**.** G is called *sem-group* if only (A1) holds, and *monoid* if (A1) and (A2) hold.

In the sequel we shall drop the $*$, i.e. write ab instead of $a * b$.

Proposition 4.3. *The identity and inverses are unique.*

Proof. Assume e and e' are two identities, i.e. satisfy

$$ex = xe = x, \quad e'y = ye' = y.$$

Then for $x = e'$ and $y = e$ we have $e' = ee' = e$. Assume now that x^{-1} and x_1^{-1} are two inverses of x, i.e.

$$x^{-1}x = xx^{-1} = e, \quad x_1^{-1}x = xx_1^{-1}.$$

Then multiplying $x^{-1}x = e$ by x_1^{-1} on the right and multiplying $xx_1^{-1} = e$ by x^{-1} on the left, we obtain $x_1^{-1} = x^{-1}xx_1^{-1} = x^{-1}$ as desired. □

If G is finite, the number of its elements is called the *order* of G, denoted by $|G|$.

4.1. **Powers of elements.** For every element g in a group G, we set $g^0 = e$, and define its positive powers inductively by

$$g^{n+1} := gg^n,$$

and the negative powers by taking the inverse

$$g^{-n} := (g^n)^{-1}.$$

Then it can be checked that

$$g^{m+n} = g^n g^m$$

for any $m, n \in \mathbb{Z}$.

4.2. **Cayley table.** The *Cayley table* for a binary operation $*$ on a set S is the table with elements of S in rows and columns, and for each $a, b \in S$, the cell in the intersection of the row of a and the column of b has the result of operation $a * b$. The Cayley table contains complete information about the binary operation.

5. Subgroups

Definition 5.1. A subset H in a group G is a *subgroup* if it is

(1) closed under the group operation, i.e. for all $a, b \in H$ one has $ab \in H$;
(2) H forms a group with respect to the restriction of the operation of G.

As direct consequence of group axioms, both G and H have identity elements. It is, however, not immediately clear that both identities are the same, which is part of the following lemma.

Lemma 5.2. *If $H \subset G$ is a subgroup, both identities in H and G must coincide and for every $h \in H$, its inverses in G and H also must coincide.*

Proof. Let e_1 be the identity in H, i.e. $e_1 h = h e_1 = h$ for all $h \in H$. Then for $h = e_1$, we have $e_1 e_1 = e_1$. Multiplying by the inverse e_1^{-1} (in G) on the right or left, we get $e_1 = e$, where e is the identity in G, proving the first statement.

Now, since both H and G have the same identity e, the inverse h^{-1} of $h \in H$ in H satisfies $h^{-1}h = hh^{-1} = e$. But the inverse h_1^{-1} of h in G has the same properties. Thus we have two inverses in G that must be equal by the uniqueness. This proves the second statement. □

Proposition 5.3. *A subset $H \subset G$ is a subgroup if and only if*

(1) *H is closed under the group operation;*
(2) *$H \neq \emptyset$;*
(3) *for every $h \in H$, its inverse h^{-1} (in G) is also in H.*

Proof. If $H \subset G$ is a subgroup, it is closed under the group operation proving (1) and contains the identity, which coincides with the identity e in G by Lemma 5.2, proving (2). Then again by the same lemma, for every $h \in H$, its inverse in H coincides with its inverse h^{-1} in G, therefore $h^{-1} \in H$ proving (3).

Vice versa, assuming (1), (2), (3), H is closed by (1). Since it is nonempty by (2), we can take some $h \in H$, then $h^{-1} \in H$ by (3) and hence $e = hh^{-1} \in H$ since H is closed. Finally (3) implies that every element in H has inverse there. Thus H is a subgroup. □

5.1. **Generators.** A natural source of subgroups those generated by some elements. A subgroup $H \subset G$ is generated by a set of elements $A \subset G$ is the intersection of all subgroups of G containing A. The latter is always a subgroups in view of the the following lemma:

Lemma 5.4. *Let G be any group. The intersection of any family $(H_\alpha)_{\alpha \in A}$ of subgroups $H_\alpha \subset G$ is a subgroup of G.*

Proof. Denote by H the intersection of $(H_\alpha)_{\alpha\in A}$. Then for any $a, b \in H$, we have $a, b \in H_\alpha$ for every α. Since H_α is subgroup, $ab \in H_\alpha$ for every α, hence $ab \in H$. That proves that H is closed under the group operation.

Since each H_α contains the identity e, H also does and is therefore nonempty. Finally, for every $a \in H$, we have $a \in H_\alpha$ implying $a^{-1} \in H_\alpha$ since H_α is a subgroup. Since α is arbitrary, this shows $a^{-1} \in H$.

The proof is completed by using Proposition 5.3. □

The following gives a complete description of the generated subgroup by a subset.

Proposition 5.5. *Let G be a group and $S \subset G$ any subset. Then the subgroup $\langle S\rangle \subset G$ generated by S consists of all words $x_1 \dots x_n$ (of any length n), where for every j, either $x_j \in S$ or $x_j^{-1} \in S$.*

Proof. Let H be the set of all words as in the proposition. Then it is clearly closed under the operation, is nonempty (contains the empty word equal to the idenity), and contains inverses of its elements, since

$$(x_1 \dots x_n)^{-1} = x_n^{-1} \dots x_1^{-1}$$

is another word. Hence H is a subgroup by Proposition 5.3.

On the other hand, any subgroup containing S must also contain all words as above, hence H is the minimal such subgroup. □

5.2. **Cyclic groups.** A group is *cyclic* if it is generated by a single element. $(\mathbb{Z}, +)$ is cyclic but $(\mathbb{Q}, +)$ is not.

As corollary of Proposition 5.5, we obtain:

Corollary 5.6. *The subgroup generated by a single element $g \in G$ consists of all integer powers g^n for $n \in \mathbb{Z}$.*

6. Permutation groups

A *permutation* of a set S is any bijective self-map of S. All permutations of a set S form the *permutation group* of S with respect to composition. In case $S = \{1, \dots, n\}$, its permutation group is also called *symmetric group* and is denoted by S_n.

Lemma 6.1. *The number of elements in S_n is $|S_n| = n!$.*

Proof. Counting the number of all possible self-bijections σ of $\{1, \dots, n\}$, we see that there are n choices for $\sigma(1)$, after which there are $(n-1)$ remaining choices for $\sigma(2)$, then $(n-2)$ remaining choices for $\sigma(3)$, and similarly, for every m, there will be $(n-m+1)$ choices for $\sigma(m)$. Combining all the choices, we obtain $n!$ possible self-bijections σ. □

Proposition 6.2. *Every permutation σ can be written as product of* transpositions*, i.e. permutations exchanging two elements. In other words, the set of all transpositions generates S_n.*

Proof. We argue by induction on n, where the statement is obvious for $n = 1, 2$. Every permutation σ of $\{1, \dots, n\}$ can be composed with the transposition σ_0 exchanging $\sigma(n)$ and n. The composition $\sigma_0\sigma$ preserves n and hence corresponds to a permutation of $\{1, \dots, n-1\}$, which by induction is a product of transpositions: $\sigma_0\sigma = \tau_1 \dots \tau_m$. Since $\sigma_0^{-1} = \sigma_0$, we obtain

$$\sigma = \sigma_0\tau_1 \dots \tau_m,$$

completing the induction step. □

6.1. **Sign of permutation and alternating group.** Consider permutations acting on variables $x_1, \dots, x_n$, and therefore on the polynomial function

$$\Delta(x_1, \dots, x_n) := \prod_{j<k}(x_j - x_k),$$

transforming it into

$$\Delta_\sigma(x_1, \dots, x_n) := \Delta(x_{\sigma(1)}, \dots, x_{\sigma(n)}).$$

If σ is a transposition exchanging two fixed numbers $i < j$, then

$$\Delta(x_1, \dots, x_n) = (x_i - x_j)\times$$

$$\prod_{k<i}(x_k - x_i)(x_k - x_j) \cdot \prod_{i<k<j}(x_i - x_k)(x_k - x_j) \cdot \prod_{k>j}(x_i - x_k)(x_j - x_k)\times$$

$$\prod_{k<l, k, l\notin\{i,j\}}(x_k - x_l).$$

Then exchanging x_i and x_j we see that the first factor changes the sign, the first, third and forth products do not change, whereas in the second product both factors change sign. Consequently the whole product changes the sign and we obtain $\Delta_\sigma = -\Delta$.

Since every permutation σ is a product of transpositions, it either transforms Δ into itself or into $-\Delta$, depending on the parity of the number of transpositions involved. That is, $\Delta_\sigma = \Delta$ if Δ is a product of even number of transpositions, and $\Delta_\sigma = -\Delta$ if Δ is a product of odd number of transpositions. Note that since Δ_σ depends only on σ but not on the way σ is represented as product of transpositions, *the number of transpositions involved is either always even or always odd.*

If $\Delta_\sigma = \Delta$ we say that the *sign* (or *signature*) $\mathsf{sgn}(\sigma) = 1$ and call σ *even*. Otherwise, when $\Delta_\sigma = -\Delta$, we call $\mathsf{sgn}(\sigma) = -1$ and σ is called *odd*. That is, for all $\sigma \in S_n$ we have the identity

$$\Delta_\sigma = \mathsf{sgn}(\sigma)\Delta.$$

Writing σ and τ as products of k and l transpositions, we conclude that $\sigma\tau$ can be written as product of $k + l$ transpositions. Hence sgn is multiplicative, i.e.

$$\mathsf{sgn}(\sigma\tau) = \mathsf{sgn}(\sigma)\,\mathsf{sgn}(\tau),$$

and the set of all even permutations forms the important *alternating subgroup* $A_n \subset S_n$.

6.2. **Cycle decompositions.** For any distinct set of integers $1 \leq a_1, \dots, a_m \leq n$, the cycle $(a_1 \dots a_m)$ is the permutation $\sigma \in S_n$ which "cycles" (i.e. permutes in cyclic order) the a_k's, i.e. sends a_k into a_{k+1} for $1 \leq k < m$ and a_m into a_1. Every permutation can be uniquely written as composition of pairwise disjoint cycles.

Every m-cycle is a product of $(m-1)$ transpositions:

$$\sigma = (a_1 \dots a_m) = (a_1 a_2)(a_2 a_3) \dots (a_{m-1} a_m).$$

In particular, it follows that its sign is $\mathsf{sgn}(\sigma) = (-1)^{m-1}$.

Example 6.3. The alternating subgroup $A_3 \subset S_3$ consists of the identity and all 3-cycles $(a_1 a_2 a_3)$. The alternating subgroup $A_4 \subset S_4$ consists of all 3-cycles $(a_1 a_2 a_3)$ and all products of disjoint 2-cycles $(a_1 a_2)(a_3 a_4)$.

7. Matrix groups

For every $n = 1, 2, \dots$, the sets of all $n \times n$ matrices over $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ form monoids under multiplication.

7.1. **General linear groups.** Their subsets of *invertible* matrices form with respect to matrix multiplication the *general linear groups*

$$\mathsf{GL}_n(\mathbb{Z}) \subset \mathsf{GL}_n(\mathbb{Q}) \subset \mathsf{GL}_n(\mathbb{R}) \subset \mathsf{GL}_n(\mathbb{C}),$$

sometimes also written as $\mathsf{GL}(n, \mathbb{Q})$ etc. Recall that a matrix A is invertible over $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ (or, more generally, over any field) if and only if $\det A \neq 0$. In case of $\mathbb{Z}$ (which is not a field), a matrix over it is invertible if and only if its determinant is invertible in $\mathbb{Z}$, i.e. either 1 or -1.

7.2. **Special linear groups.** Important subgroups of general linear groups are *special linear groups*

$$\mathsf{SL}_n(\mathbb{Z}) \subset \mathsf{SL}_n(\mathbb{Q}) \subset \mathsf{SL}_n(\mathbb{R}) \subset \mathsf{SL}_n(\mathbb{C}),$$

consisting of corresponding matrices with determinant 1.

7.3. **Orthogonal and unitary groups.** Further important subgroups of general linear groups are *orthogonal groups*

$$\mathsf{O}_n(\mathbb{Z}) \subset \mathsf{O}_n(\mathbb{Q}) \subset \mathsf{O}_n(\mathbb{R}) \subset \mathsf{O}_n(\mathbb{C}),$$

consisting of corresponding matrices A with $AA^t = \mathsf{id}$, where A^t is the transpose matrix, and the *unitary group*

$$\mathsf{U}_n = \mathsf{U}_n(\mathbb{C})$$

consisting of all *complex* matrices A with $A\bar{A}^t = \mathsf{id}$, where $\bar{A}$ is the complex conjugate. Note that the unitary group is only interesting to consider over $\mathbb{C}$, where $\bar{A} \neq A$, which is why it is usually simply written as U_n or $U(n)$.

Recall that orthogonal matrices are precisely those preserving the standard euclidean scalar product

$$(x, y) = x_1 y_1 + \dots + x_n y_n,$$

and unitary matrices are those preserving the standard hermitian scalar product

$$\langle x, y\rangle = x_1\bar{y}_1 + \ldots + x_n\bar{y}_n.$$

7.4. **Special orthogonal and unitary groups.** Intersecting orthogonal and unitary groups with special linear groups one obtains *special orthogonal groups* and *special unitary group*

$$\mathsf{SO}_n(\mathbb{Z}) \subset \mathsf{SO}_n(\mathbb{Q}) \subset \mathsf{SO}_n(\mathbb{R}) \subset \mathsf{SO}_n(\mathbb{C}), \quad \mathsf{SU}_n,$$

$$\mathsf{SO}_n(\mathbb{K}) := \mathsf{O}_n(\mathbb{K}) \cap \mathsf{SL}_n(\mathbb{K}), \quad \mathsf{SU}_n := \mathsf{U}_n \cap \mathsf{SL}_n(\mathbb{C})$$

8. Binary and equivalence relations

A *binary relation* on a subset S is any subset $\mathcal{R} \subset S \times S$, i.e. subset of pairs of elements of S. We write $a \sim b$ whenever $(a, b) \in \mathcal{R}$ and call $\sim$ the (binary) relation. A (binary) relation $\sim$ is an *equivalence relation* if it is reflexive, symmetric and transitive.

Let $\sim$ be an equivalence relation on S. For every $a \in S$, its *equivalence class* is the subset of all $x \in S$ with $x \sim a$. For every equivalence relation on S there is unique *partition* of S into equivalence classes, i.e. decomposition of S as union of pairwise disjoint equivalence classes.

9. Integer division, greatest common divisor and congruences

9.1. **Integer division with remainder.** Given $m, n \in \mathbb{Z}$ with $n > 0$, there exist unique $q, r \in \mathbb{Z}$ satisfying

$$m = nq + r, \quad 0 \leq r < n.$$

Indeed, it suffices to take $q = [m/n]$, the integral part of m/n, i.e. the maximal integer not greater than m/n, and set $r := m - nq$.

If $r = 0$, i.e. $n = mq$, m is said to *divide* n or to be a *divisor* of n, and n is said to be *divisible* by m.

9.2. **Application: additive sugroups of $\mathbb{Z}$.**

Theorem 9.1. *Additive subgroups $H \subset \mathbb{Z}$ are precisely those given by $H = n\mathbb{Z}$ for $n = 0, 1, \ldots$.*

Proof. For $H \neq \{0\}$, take $n > 0$ to be the minimal positive element of H. Then any other $h \in H$ can be divided by n with remainder r, which also must belong to H and is therefore 0. Thus $H = n\mathbb{Z}$. □

9.3. **Greatest common divisor.** The *greatest common divisor* $\gcd(m, n)$ of two positive integers m, n is the largest positive integer k which divides both m and n. If $\gcd(m, n) = 1$, the integers m and n are said to be *relatively prime* or *coprime*.

Theorem 9.2. *The greatest common divisor k of m and n can be written as integer linear combination $k = am + bn$, $a, b \in \mathbb{Z}$.*

The proof is by the Euclidean algorithm.

9.4. **Unique prime factorization.** Recall that an integer $p \neq \pm 1$ is *prime* if its only divisors are $\pm 1, \pm p$.

Lemma 9.3. *If a prime p divides mn, then p divides either m or n.*

Proof. Suppose p divides mn but not m. Then $\gcd(p, m) = 1$ and by Theorem 9.2,

$$1 = ap + bm.$$

Multiplying by n we obtain $n = anp + bnm$. Since p divides bnm and anp, it also divides n as desired. □

Theorem 9.4 (Unique prime factorization)**.** *Every integer $n \geq 2$ can be expressed as a product of (positive) prime numbers (not necessarily distinct),*

$$n = p_1 \cdots p_r,$$

uniquely determined up to a permutation.

Proof. We show existence of prime decomposition by induction on n. It clearly holds for $n = 2$. Now given any n, it is either prime, in which case n is the only prime factor itself, or $n = pq$ for some integers $1 < p, q < n$. By induction, both p and q are decomposable as product of primes, and hence n also is.

We now show the uniqueness again by induction on n. It clearly holds for $n = 2$. Suppose n has two prime decompositions:

$$n = p_1 \cdots p_r = q_1 \cdots q_s.$$

Then the prime p_1 divides $q_1 \cdots q_s$ and using Lemma 9.3 repeatedly, we see that p_1 must divide one of q_j, say q_1. But since q_1 is also prime, $p_1 = q_1$ and hence

$$n' = p_2 \cdots p_r = q_2 \cdots q_s.$$

Since $n' < n$, it has unique prime decomposition by induction and therefore n does. □

9.5. **Congruences modulo n.** Two integers m, k are *congruent modulo n* if $m - k$ is divisible by k, written

$$m \equiv k \mod n.$$

It follows from integer division with remainder that every m is congruent to precisely one integer between 0 and $n - 1$.

One verifies that congruence is an equivalence relation, whose equivalence classes are called *congruence classes* $[m]$. Denote by $\mathbb{Z}_n$ the set of all congruence classes modulo n. Then the addition and multiplication of integers induce well-defined addition and multiplication on $\mathbb{Z}_n$. Then $(\mathbb{Z}_n, +)$ becomes a group, and $(\mathbb{Z}_n, \cdot)$ a monoid.

9.6. **The group of units of a monoid.** By definition, if S is a monoid, S^* is the subset of all invertible elements (also called *units*), i.e. elements having inverses. Since $(ab)^{-1} = b^{-1}a^{-1}$ and $(a^{-1})^{-1} = a$, S^* is closed under the operation of S and is a group with respect to this operation, called the *group of units of the monoid*.

9.7. **Multiplicative group $\mathbb{Z}_n^*$.**

Lemma 9.5. *A congruence class $[m] \in \mathbb{Z}_n$ is invertible if and only if $\gcd(m,n) = 1$ (i.e. m and n are coprime).*

Proof. If $[m]$ is invertible and $[l]$ is its inverse, we have $ml = 1 \mod n$, i.e. $ml + nk = 1$ for some integer k, implying $\gcd(m,n) = 1$.

Vice versa, $\gcd(m,n) = 1$ implies $1 = am + bn$ for some $a, b \in \mathbb{Z}$ by Theorem 9.2, i.e. $am = 1 \mod n$, and hence $[m]$ is invertible in $\mathbb{Z}_n$. □

Thus the group of units $\mathbb{Z}_n^*$ consists of all $[m]$ such that m is coprime with n. More specially, if $n = p$ is prime, any m is either divisible by p or coprime with it. Hence we obtain:

Lemma 9.6. *If p is prime, $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{[0]\}$.*

10. Cosets, orders of elements, and Largrange's Theorem

10.1. **Cosets.** Cosets are generalizations of congruence classes. Given a group G and a subgroup $H \subset G$, its left and right cosets are respectively subsets gH and Hg for any $g \in G$.

Example 10.1. For the subgroup $H = n\mathbb{Z} \subset \mathbb{Z}$, its both left and right cosets are congruence classes $gH = Hg = [g]$.

Also in general cosets are equivalence classes where $a \sim b$ whenever $aH = bH$ for right cosets and whenever $Ha = Hb$ for left cosets.

10.2. **Group and element orders.** The *order* $|G|$ of a group G is the (possibly infinite) number of elements. For every element $g \in G$, define its *order* to be the order of the subgroup generated by g.

Example 10.2. The symmetric group S_n has order $n!$. Its alternating subgroup $A_n \subset S_n$ of all even permutations has two cosets A_n and σA_n with equal number of elements, where σ is any odd permutation. Hence $|A_n| = n!/2$.

Theorem 10.3. *The subgroup generated by g consists precisely of all powers g^k. Let $n \geq 0$ be either the minimum n with $g^n = e$, or ∞ if $g^k \neq e$ for all $k \geq 1$. Then $g^k = g^m$ if and only if $k \equiv m \mod n$ (or $k = m$ for $n = \infty$). The order of g equals n.*

10.3. **Langrange's Theorem.**

Theorem 10.4. *If G is a finite group and $H \subset G$, the order of H divides the order of G.*

Corollary 10.5. *In a finite group G, the order of every element divides the order of G. Consequently $g^{|G|} = e$ for every $g \in G$.*

10.4. **Fermat's little theorem.**

Theorem 10.6. *If p is prime and $x \not\equiv 0 \mod p$, then $x^{p-1} \equiv 1 \mod p$.*

Proof. By Lemma 9.6, $|\mathbb{Z}_p^*| = p - 1$ and the theorem follows from Corollary 10.5. □

An equivalent version is:

Theorem 10.7. *If p is prime, then $x^p \equiv x \mod p$ for all x.*

11. Homomorphisms

11.1. **Group homomorphisms, isomorphisms, and their kernels.** A map $f\colon G \to G'$ between two groups is a *(group) homomorphism* if it sends products into products, i.e. $f(ab) = f(a)f(b)$. It follows that $f(e) = e$ and $f(a^{-1}) = (f(a))^{-1}$. Image $f(G) \subset G'$ of homomorphism is always a subgroup of G'.

Isomorphism is a bijective homomorphism.

The *kernel* $\ker f$ of a homomorphism $f\colon G \to G'$ is the preimage of the identity $e \in G'$.

Theorem 11.1. *The kernel $H := \ker f$ of a group homomorphism is a subgroup of G such that*

$$gHg^{-1} \subset H \tag{11.1}$$

for every $g \in G$.

11.2. **Normal subgroups.** A subgroup $H \subset G$ satisfying (11.1) for all $g \in G$ is called *normal subgroup*, written $H \lhd G$.

11.3. **Quotient group modulo normal subgroup.** Let $H \lhd G$ be a normal subgroup.

Lemma 11.2. *Then $gH = Hg$ for all $g \in G$, i.e. right and left cosets are the same.*

Theorem 11.3. *The group operation on G induces a well-defined group operation on the set of all right (and hence left) H-cosets.*

The group of all right (or left) H-cosets in G is called the *quotient group* G/H.

11.4. **First isomorphism theorem.**

Theorem 11.4. *Let $f\colon G \to G'$ be any homomorphism and let $H := \ker f$. Then f induces the group isomorphism*

$$\widetilde{f}\colon G/H \to f(G), \quad gH \mapsto f(g).$$

Proof. By definition of $\ker f$, the map $\widetilde{f}$ is well-defined, i.e. $f(g)$ depends only on the class gH. Since f is homomorphism, so is $\widetilde{f}$. It is clearly surjective and also injective: if $\widetilde{f}(gH) = \widetilde{f}(g'H)$, then $f(g^{-1}g') = e$ implying $g^{-1}g' \in H$, i.e. $g'H \subset gH$ and $gH \subset g'H$ by symmetry. Hence $\widetilde{f}$ is an isomorphism. □

11.5. **Chinese Remainder Theorem.**

Theorem 11.5 (Chinese Remainder Theorem)**.** *Let $n_1, \dots, n_k$ be nonzero integers that are pairwise coprime (i.e. no two have common divisor other than ± 1). Then for any integers $l_1, \dots, l_k$ there exists an integer m satisfying*

$$m \equiv l_j \mod n_j, \quad j = 1, \dots, k.$$

Proof. Consider the direct product $G := \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ and the homomorphism

$$f \colon \mathbb{Z} \to G, \quad m \mapsto ([m]_{n_1}, \dots, [m]_{n_k}).$$

We need to prove that f is surjective. Consider unique prime decompositions of m and each n_j. Since n_j are pairwise coprime, no prime can appear in factorization of more than one n_j. If $m \in \ker f$, i.e. it is divisible by each n_j, each factor p appearing with power p^k in factorization of any n_j must divide m. Hence the factorization of m contains those factors and hence m is divisible by the product of all such p^k, i.e. by the product

$$n := n_1 \cdots n_k.$$

It follows that $\ker f = n\mathbb{Z}$ and by the first isomorphism theorem, the image subgroup $f(\mathbb{Z})$ is isomorphic to the quotient $\mathbb{Z}/\ker f = \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$. Then $|f(\mathbb{Z})| = n = |G|$ implying surjectiviity of f as desired. □

12. Group actions on sets

12.1. **Definitions and elementary properties.**

Definition 12.1. An action of group G on a set S is a group homomorphism f from G into the group $\mathsf{Sym}(S)$ of all permutations (bijective self-maps) of S. If f is injective, the action is called *faithful*.

The common notation is

$$g \cdot x = f(g)(x), \quad g \in G,\ x \in S. \tag{12.1}$$

Proposition 12.2. *Given an action $f \colon G \to \mathsf{Sym}(S)$, we have*

1. *$e \cdot x = x$ (where e is the identity in G);*
2. *$(gh) \cdot x = g \cdot (h \cdot x)$.*

Vice versa, any map $G \times S \to S$, $(g, x) \mapsto g \cdot x$, satisfying (1) and (2), defines an action $f \colon G \to \mathsf{Sym}(S)$ such that (12.1) *holds.*

Definition 12.3. The *stabilizer* of $x \in S$ is defined by

$$G_x := \{g \in G : g \cdot x = x\}.$$

The *orbit* of $x \in S$ is defined by

$$G \cdot x := \{g \cdot x : g \in G\}.$$

Lemma 12.4. *For any action, we have:*

(1) *The stabilizer G_x is always a subgroup of G.*
(2) *Different orbits do not intersect. In fact, being in the same orbit defines an equivalence relation on S with orbits being equivalence classes.*

In the following, for any subgroup $H \subset G$, denote by G/H the set of all left H-cosets $gH \subset G$.

Example 12.5. For any subgroup $H \subset G$, G naturally acts on the set G/H of left H-cosets. The action is defined by

$$G \times G/H \to G/H, \quad (g, g_1H) \mapsto g \cdot g_1H := gg_1H.$$

For every class $x = g_0H \in G/H$, its stabilizer is

$$G_x = \{g : g \cdot x = x\} = \{g : gg_0H = g_0H\} = \{g : gg_0 \in g_0H\} = \{g : g \in g_0Hg_0^{-1}\} = g_0Hg_0^{-1}.$$

In particular, if $g_0 = e$, we have $G_x = H$, i.e. any subgroup H is realized as a stabilizer of some group action of G.

Theorem 12.6. *For each $x \in S$, the map $f\colon [g] \mapsto g \cdot x$ induces a bijection $G/G_x \to G \cdot x$. In particular, if G is finite, any orbit $G \cdot x$ is finite and we have*

$$|Gx| = \frac{|G|}{|G_x|}.$$

Proof. The map f is well-defined: if $g_1 \in [g] \in G/G_x$ is another representative, we have $g_1 = gh$, $h \in G_x$, and hence

$$g_1 \cdot x = gh \cdot x = g \cdot (h \cdot x) = g \cdot x,$$

since G_x is the stabilizer of x.

Further, f is injective: if $g \circ x = g_1 \circ x$, then $g^{-1}g_1 \cdot x = x$ implying $g^{-1}g_1 \in G_x$, i.e. $[g_1] = [g]$ in G/G_x.

Finally, f is clearly surjective by definition of the orbit $G \cdot x$. This shows that f is bijective. □

13. Cayley's theorem

Theorem 13.1 (Cayley's theorem)**.** *Every group is isomorphic to a subgroup of the permutation group $\mathsf{Sym}(S)$ for some set S.*

Proof. Consider the action of G on itself by left multiplication:

$$g \cdot x = gx, \quad g, x \in G.$$

This is clearly an action and the resulting homomorphism $f\colon G \to \mathsf{Sym}(G)$, $g \mapsto (x \mapsto gx)$ has zero kernel. Hence by First Isomorphism Theorem, f is an isomorphism onto its image, which is a subgroup of the permutation group of G as desired. □

14. Sylow's 1st theorem

By Lagrange's theorem, the order of any subgroup $H \subset G$ divides the order of $|G|$. On the other hand, in general, for a divisor d of $|G|$, there may be no subgroups $H \subset G$ of order d.

Example 14.1. Let $G = A_4$ be the alternating group of all even permutations of order 4, whose order is $|S_4|/2 = 4!/2 = 12$. It consists of all permutations having disjoint cycle decompositions either $(a_1a_2)(b_1b_2)$ or $(a_1a_2a_3)$. What are possible subgroups $H \subset G$?

We clearly have subgroups $H = \{e, (a_1a_2)(b_1b_2)\}$ of order 2 (generated by $(a_1a_2)(b_1b_2)$) and $H = \{e, (a_1a_2a_3), (a_1a_3a_2)\}$ of order 3 (generated by $(a_1a_2a_3)$). Clearly all subgroups of order 2 and 3 are of this kind.

Assume now H has order ≥ 4. If H contains an element $h_0 = (a_1a_2a_3)$ and $h_1 = (b_1b_2)(c_1c_2)$, then switching b_i with c_i, if necessary, we may assume $b_1, b_2 \in \{a_1, a_2, a_3\}$. Further, cycling a_1, a_2, a_3 and switching b_1, b_2, if necessary, we may assume $h_1 = (a_1a_2)(a_3a_4)$. Then H also contains

$$h_2 := h_0h_1h_0^{-1} = (a_2a_3)(a_1a_4), \quad h_3 := h_0^2h_1h_0^{-2} = (a_1a_3)(a_2a_4),$$

i.e. all possible products of 2 disjoint cycles.

Next H contains $h_1h_0h_1^{-1} = (a_2a_1a_4)$, and hence also $(a_2a_1a_4)^{-1} = (a_1a_2a_4)$. Analogously, H contains $h_2h_0h_2^{-1} = (a_4a_3a_2)$ and $h_3h_0h_3^{-1} = (a_3a_4a_1)$ and its inverses, hence all 3-cyles. Summarizing, we must have $H = A_2$.

The remaining possibility are that H only has 3-cycles or only products of 2-cycles.

In the first case, H has two 3-cycles $(a_1a_2a_3)$ and $(b_1b_2b_3)$ with $\{a_1, a_2, a_3\} \neq \{b_1, b_2, b_3\}$, then we may assume that $a_2, a_3 \in \{b_1, b_2, b_3\}$ and set $a_4 := b_3$. In that case we have $(a_1a_2a_3)(a_2a_3a_4) = (a_1a_2)(a_3a_4) \in H$. Now the above argument shows $H = A_2$.

Finally, the last possibility is H having only products of 2-cycles, of which we must have at least two that we can write as $h_1 = (a_1a_2)(a_3a_4)$ and $h_2 = (a_1a_3)(a_2a_4)$. Then H also contains $h_1h_2 = (a_1a_4)(a_2a_3)$, in which case

$$H = \{e, (12)(34), (13)(24), (14)(23)\},$$

which is the only subgroup of order 4.

Thus A_4 has subgroups of orders $1, 2, 3, 4$ and 12. However, it does not have any subgroup of order 6 which is a divisor of $|A_4|$.

Writing the prime decomposition $|A_2| = 2^2 \cdot 3$, we find subgroups of orders 1, 2, 2^2, 3, and $2^2 \cdot 3$, i.e. we have subgroups of orders p^k whenever p is prime and p^k divides 12, but not necessarily of an order $p_1^{k_1}p_2^{k_2}$ with p_1, p_2 different primes.

Definition 14.2. If p is a prime, any subgroup $H \subset G$ of order $|H| = p^k$ for some k is called a *p-subgroup*. By Lagrange's theorem, p^k divides the order $|G|$. If k is maximal such that p^k divides $|G|$, any H of order $|H| = p^k$ is called *Sylow p-subgroup*.

Theorem 14.3. *If G is finite group whose order is divisible by p^k, where p is prime, then G has a subgroup of order p^k.*

For k maximal with p^k dividing $|G|$, we obtain the Sylow's 1st theorem: G has a Sylow p-subgroup for every prime p dividing $|G|$.

Proof (Wielandt, 1959). Let S be the set of all p^k-element subsets of G. We can write $|G| = p^l m$ such that m is not divisible by p. Then S consists of

$$\binom{mp^l}{p^k} = \frac{p^l m(p^l m - 1)\cdots(p^l m - p^k + 1)}{p^k(p^k - 1)\cdots 1} \tag{14.1}$$

elements. The latter number is equal to the product of m and the fractions

$$\frac{p^l m - j}{p^k - j}, \quad 0 < j < p^k. \tag{14.2}$$

For each j, let p^s be the highest power of p dividing $p^l m - j$. Then $s < k$, since otherwise j would be divisible by p^k which contradicts $0 < j < p^k$. Now since p^s divides $p^k m$, it also divides j and hence $p^k - j$. Vice versa, if p^s divides $p^k - j$, we must have $s < k$ and hence p^s divides j implying that it divides $p^k m - j$. Summarizing, we obtain that powers of p in the factorization of both numerator and denominator in (14.2) are the same and hence the right-hand side in (14.1) is not divisible by p^{l-k+1}. Consequently, also the number $|S|$ of elements of S is not divisible by p^{l-k+1}.

Consider the action of G on S given by

$$g \cdot \{g_1, \dots, g_{p^k}\} := \{gg_1, \dots, gg_{p^k}\}.$$

Since S is a disjoint union of G-orbits and the number of elements of S is not divisible by p^{l-k+1}, there exists at least one orbit $G \cdot x$ with

$$x = \{g_1, \dots, g_{p^k}\}$$

such that the number of elements $|G \cdot x|$ is not divisible by p^{l-k+1}. By Theorem 12.6,

$$|G_x| = |G|/|G \cdot x| = mp^l/|G \cdot x|$$

is divisible by p^k. On the other hand, if $g \in G_x$, then

$$\{gg_1, \dots, gg_{p^k}\} = \{g_1, \dots, g_{p^k}\}$$

and hence $gg_1 = g_j$ for some $j = 1, \dots, p^k$, i.e. $g = g_1^{-1} g_j$, implying $|G_x| \le p^k$. Hence $|G_x| = p^k$. Since the stabilizer G_x is always a subgroup of G, we obtain the desired conclusion. □

Applying Theorem 14.3 with $k = 1$, we obtain:

Corollary 14.4 (Cauchy's Theorem, 1845)**.** *If G is a finite group whose order is divisible by a prime p, then G contains an element of order p.*

15. Classification of finite abelian groups

Recall that for every groups $G_1, \dots, G_r$, their *direct product* $G_1 \times \dots \times G_r$ is defined as their cartesian product with component-wise multiplication, i.e.

$$(g_1, \dots, g_r)(h_1, \dots, h_r) := (g_1 h_1, \dots, g_r h_r),$$

or, when all groups are abelian, in the additive notation,

$$(g_1, \dots, g_r) + (h_1, \dots, h_r) := (g_1 + h_1, \dots, g_r + h_r).$$

For abelian groups, their direct product is also called *direct sum* written as

$$G_1 \oplus \dots \oplus G_r.$$

Lemma 15.1. *If G is abelian group and $H_1, H_2 \subset G$ are finite subgroups with $\gcd(|H_1|, |H_2|) = 1$, then the map*

$$f \colon H_1 \oplus H_2 \to H, \quad (h_1, h_2) \mapsto h_1 + h_2$$

is an injective homomorphism.

Proof. If $h = (h_1, h_2) \in \ker f$, then $h_1 = -h_2$ and hence $h_1 \in H_1 \cap H_2$. By Corollary 10.5, the order of h_1 divides both $|H_1|$ and $|H_2|$ implying $h_1 = 0$ and then $h_2 = 0$. Hence $\ker f = \{0\}$ proving injectivity of f. □

Corollary 15.2. *For every decomposition $n = n_1 n_2$ with $\gcd(n_1, n_2) = 1$, the cyclic group $\mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$.*

By induction, Lemma 15.1 can be generalized as follows:

Lemma 15.3. *If G is abelian group and $H_j \subset G$, $j = 1, \dots, r$, are finite subgroups with $|H_j|$ pairwise coprime, then the map*

$$f \colon H_1 \oplus \dots \oplus H_r \to H, \quad (h_1, \dots, h_r) \mapsto h_1 + \dots + h_r$$

is an injective homomorphism.

Proof. The proof is by induction on r. The case $r = 2$ is treated in Lemma 15.1. Now given any r, set

$$H'_{r-1} := H_1 + \dots + H_{r-1} \subset H.$$

Since the map

$$H_1 \oplus \dots \oplus H_{r-1} \to H, \quad (h_1, \dots, h_{r-1}) \mapsto h_1 + \dots + h_{r-1}$$

is injective by the induction assumption, $|H'_{r-1}| = |H_1| \cdots |H_{r-1}|$ and hence $|H'_{r-1}|$ and $|H_r|$ are coprime and we can use again Lemma 15.1 for H'_{r-1} and H_r to obtain the desired conclusion. □

Corollary 15.4. *Let $n = p_1^{k_1} \cdots p_r^{k_r}$ be the prime decomposition of n with $p_i \neq p_j$ and $k_j > 0$. Then $\mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_{p_1^{k_1}} \oplus \dots \oplus \mathbb{Z}_{p_r^{k_r}}$.*

Lemma 15.5. *Let G be an abelian group generated by elements $x_1, \dots, x_k$. For any $c_1, \dots, c_k \in \mathbb{N}_{\geq 0}$ with $\gcd(c_1, \dots, c_k) = 1$, there exist generators $y_1, \dots, y_k$ of G (i.e. $G = \langle y_1, \dots, y_k \rangle$) such that $y_1 = c_1 x_1 + \dots + c_k x_k$.*

Proof. We argue by induction on $s := c_1 + \dots + c_k$. The lemma is clear for $s = 1$ (with y_j's obtained by permutation of the x_j's). Otherwise for $s > 1$, after possibly exchanging x_1, x_2, we may assume $c_1 \geq c_2 > 0$. Now apply the induction for the set of generators $x_1, x_2 + x_1, x_3, \dots, x_k$ and the numbers $c_1 - c_2, c_2, c_3 \dots, c_k \in \mathbb{N}_{\geq 0}$. Since

$$\gcd(c_1 - c_2, c_2, c_3 \dots, c_k) = 1$$

and

$$(c_1 - c_2) + c_2 + c_3 + \dots + c_k < c_1 + c_2 + c_3 + \dots + c_k = s,$$

by induction, there exist generators $y_1, \dots, y_k$, such that

$$y_1 = (c_1 - c_2)x_1 + c_2(x_1 + x_2) + c_3 x_3 + \dots + c_k x_k = c_1 x_1 + c_2 x_2 + c_3 x_3 + \dots + c_k x_k$$

as desired. □

Definition 15.6. A subset $\{x_1, \dots, x_k\}$ of an abelian group G is called a *basis* if it generates G and for $m_1, \dots, m_k \in \mathbb{Z}$, one has

$$m_1 x_1 + \dots + m_k x_k = 0 \quad \Longrightarrow \quad m_1 x_1 = \dots = m_k x_k = 0. \tag{15.1}$$

Note that a single nonzero generator x (if it exists), forms a single-element basis $\{x\}$ as (15.1) is trivial for $k = 1$.

Examples 15.7.

(1) For $G = \mathbb{Z}$, the possible bases are one-element sets $\{1\}$ and $\{-1\}$. Indeed, a basis cannot have 0 and for any nonzero integers $x_1 \neq x_2$, there exists the relation $x_2 x_1 - x_1 x_2 = 0$ violating (15.1).

(2) For $G = \mathbb{Z}_n$, each one-element set $\{[z]\} \subset \mathbb{Z}_n$, where $\gcd(z, n) = 1$, forms a basis. Indeed, since any such z is invertible in $\mathbb{Z}_n^*$ by Lemma 9.5, it generates $\mathbb{Z}_n$ and hence $\{[z]\}$ is a basis.

(3) For $G = \mathbb{Z}_6$, the set $B := \{[2], [3]\}$ is a basis. Indeed, $[1] = [3] - [2]$ is a generator, hence B generates G. Further, an identity $m_1[2] + m_2[3] = [0]$ in G implies that $2m_1 + 3m_2$ is divisible by 6 and hence m_1 and m_2 are divisible by 3 and 2 respectively, i.e. $m_1[2] = m_2[3] = [0]$ in G, proving (15.1). In particular, the number of elements in a basis is not independent of the choice of a basis, compare with Corollary 15.2.

Theorem 15.8. *Every finitely generated abelian group G has a basis.*

Proof (from Lecture Notes by J.S.Milne, http://www.jmilne.org/math/CourseNotes/GT.pdf*).* We argue by induction on the number of generators of G. If G is generated by one element, it is cyclic and the statement is clear.

Assume now that $\{x_1, \dots, x_k\}$ is a set of generators with minimal possible $k > 1$. Among such sets of generators, choose one with x_1 having the smallest possible order $|x_1|$. We claim that

$$\langle x_1 \rangle \cap \langle x_2, \dots, x_k \rangle = \{0\}. \tag{15.2}$$

Indeed, suppose that the above intersection contains a nonzero element $m_1x_1 \neq 0$, and hence we have a relation

$$m_1x_1 + m_2x_2 + \ldots + m_kx_k = 0.$$

After possibly changing the sign of some of the x_j, we may assume that $m_1, \ldots, m_k \in \mathbb{N}_{\geq 0}$. Also, replacing m_1 with its remainder modulo $|x_1|$ (the order of x_1), we may assume $m_1 < |x_1|$.

Let $d := \mathsf{gcd}(m_1, \ldots, m_k)$ and $c_i := m_i/d$. Then $\mathsf{gcd}(c_1, \ldots, c_k) = 1$ and by Lemma 15.5, there exists a set of generators $\{y_1, \ldots, y_k\}$ with $y_1 = c_1x_1 + \ldots + c_kx_k$. Then

$$dy_1 = m_1x_1 + m_2x_2 + \ldots + m_kx_k = 0,$$

hence y_1 has order at most $d \leq m_1 < |x_1|$. This is a contradiction with our choice of generators with the smallest possible $|x_1|$, proving the claim (15.2).

Since the subgroup $\langle x_2, \ldots, x_k\rangle \subset G$ has fewer generators, it has a basis $\{y_1, \ldots, y_s\}$ by induction. Then in view of (15.2), $\{x_1, y_1, \ldots, y_s\}$ is a basis of G. □

Corollary 15.9. *Every finitely generated group G is isomorphic to a direct sum of finitely many cyclic subgroups of G.*

Proof. By Theorem 15.8, G has a basis $\{x_1, \ldots, x_k\}$. Then the map

$$(m_1, \ldots, m_k) \mapsto m_1x_1 + \ldots + m_kx_k$$

defines a surjective homomorphism f from

$$\mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}, \quad n_j := |x_j|,$$

onto G, where we use the convention

$$\mathbb{Z}_\infty := \mathbb{Z}$$

for the case some of the orders $|x_j|$ are infinite. Furthermore, it follows from the definition of basis that the kernel of f is zero. Now the statement follows from the First Isomorphism Theorem. □

Definition 15.10. The *torsion subgroup* G_T in an abelian group G is the subgroup consisting of all elements of finite order.

It is easy to see that G_T is indeed a subgroup of G and in any decomposition of G as direct sum of cyclic subgroups, G_T equals the sum of all those subgroups that are finite.

Theorem 15.11. *Let $n = p_1^{k_1} \cdots p_r^{k_r}$ be the prime decompositions with $p_i \neq p_j$ and $k_j > 0$. Then every abelian group of order n is isomorphic to a direct sum of finitely many cyclic groups $\mathbb{Z}_{p_j^t}$ with $t \leq k_j$.*

Proof. Let G be abelian group of order n. By Corollary 15.9, it is isomorphic to a direct product of finitely many cyclic subgroups $\mathbb{Z}_{n_j}$. Since each n_j divides n, the desired conclusion follows from Corollary 15.4. □

Remark 15.12. Note that the group in Theorem 15.11 does not need to be a direct product of the cyclic groups $\mathbb{Z}_{p_j^{k_j}}$ (with maximal k_j), e.g. $\mathbb{Z}_2 \times \mathbb{Z}_2$ is of order $4 = 2^2$ but is not cyclic.

In view of Corollaries 15.2 and 15.4, a decomposition of G into a product of cyclic groups is not unique in general. However, we have:

Theorem 15.13. *Let G be a finitely generated abelian group. Then in any decomposition of G into a direct sum of cyclic groups, the number r of factors $\mathbb{Z}$ is an invariant depending only G.*

The number r in Theorem 15.13 is called the *rank* of G.

Proof. Let

$$G \cong \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_s} \times \mathbb{Z}^r$$

be any direct product decomposition with all n_j finite. Then the torsion subgroup $G_T = \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_s}$ is uniquely determined by G and the quotient group G/G_T, which is also uniquely determined by G, is isomorphic to $\mathbb{Z}^r$.

It remains to prove that $\mathbb{Z}^r$ cannot be isomorphic to $\mathbb{Z}^k$ for $r \neq k$. Otherwise, assuming without loss of generality $r < k$, we obtain a basis B of r elements in $\mathbb{Z}^k$. Then B would also span $\mathbb{Q}^k$ considered as vector space over $\mathbb{Q}$. However, every set that spans $\mathbb{Q}^k$ must have at least $k > r$ elements, which is a contradiction. □

D. Zaitsev: School of Mathematics, Trinity College Dublin, Dublin 2, Ireland
E-mail address: zaitsev@maths.tcd.ie