Course 7: 05.04.2021

1.11 Classification of groups of small order (not for exam)

Open problem. For a given $n \in \mathbb{N}^*$, determine all groups of order n (up to isomorphism!).

Remark 1.11.1 There is a complete classification of all finite *simple* groups.

Remark 1.11.2 (1) For every $n \in \mathbb{N}^*$, there is a group of order n, namely $(\mathbb{Z}_n, +)$.

(2) By Lagrange's Theorem, for every prime p, every group of order p is cyclic, hence abelian.

(3) By (1) and (2), for every prime p, there is a unique (up to isomorphism) group of order p, namely $(\mathbb{Z}_p, +)$.

For finite *abelian* groups there are the following general theorems.

Theorem 1.11.3 *Any finite abelian group G is isomorphic to a finite direct product of cyclic groups of prime-power order. Moreover, this decomposition is essentially unique in the sense that any two such decompositions for G have the same number of non-trivial factors of each order.*

Theorem 1.11.4 *Let G be a finite abelian group. Then G can be uniquely expressed as a direct product*

$$G \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k},$$

where $n_1, n_2, \dots, n_k$ are natural numbers such that n_{i+1} divides n_i for every $i \in \{1, 2, \dots, k-1\}$.

Example 1.11.5 *Let us determine all (non-isomorphic) abelian groups of orders* 8, 9 *and* 72.

Order 8: $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.
Order 9: $\mathbb{Z}_9$, $\mathbb{Z}_3 \times \mathbb{Z}_3$.
Order 72 (here the two isomorphic writings correspond to the above two theorems respectively):
- $\mathbb{Z}_8 \times \mathbb{Z}_9 \cong \mathbb{Z}_{72}$
- $\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \cong \mathbb{Z}_{24} \times \mathbb{Z}_3$
- $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \cong \mathbb{Z}_{36} \times \mathbb{Z}_2$
- $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \cong \mathbb{Z}_{12} \times \mathbb{Z}_6$
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \cong \mathbb{Z}_{18} \times \mathbb{Z}_2 \times \mathbb{Z}_2$
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \cong \mathbb{Z}_6 \times \mathbb{Z}_6 \times \mathbb{Z}_2$

Note that if $m, n \in \mathbb{N}$, $m, n \geq 2$ and $(m, n) = 1$, then $(\mathbb{Z}_m \times \mathbb{Z}_n, +) \cong (\mathbb{Z}_{mn}, +)$.

Example 1.11.6 *Let us determine all (non-isomorphic) groups of order* 4.

Let $(G, \cdot)$ be a group of order 4, say $G = \{e, a, b, c\}$.
Case I. If $(G, \cdot)$ has an element of order 4, then $(G, \cdot)$ is cyclic, and so $(G, \cdot) \cong (\mathbb{Z}_4, +)$.
Case II. Assume that G does not have elements of order 4. Then by Lagrange's Theorem, we must have $ord(a) = ord(b) = ord(c)$ (the order of every element of G divides the order of G). Then the operation table of G can be completed in a unique way (check it!). A model for such a group is $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ (Klein's group).

In conclusion, for every group $(G, \cdot)$ of order 4, we have either $(G, \cdot) \cong (\mathbb{Z}_4, +)$ or $(G, \cdot) \cong (\mathbb{Z}_2 \times \mathbb{Z}_2, +)$. Note that $(\mathbb{Z}_4, +) \ncong (\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ (one of them is cyclic and the other one is not).

Example 1.11.7 *Let $(G, \cdot)$ be a group. Then:*
(i) If every element of $G \setminus \{1\}$ has order 2*, then G is abelian.*
(ii) If G is finite and every element of $G \setminus \{1\}$ has order 2*, then the order of G is a power of* 2.

(i) Let $x, y \in G$. By hypothesis, we have $ord(x) = 2$, $ord(y) = 2$ and $ord(xy) = 2$. Then $(xy)^2 = 1$, hence $(xy)^{-1} = xy$. It follows that $y^{-1}x^{-1} = xy$. But $x^2 = 1$ and $y^2 = 1$ imply that $x^{-1} = x$ and $y^{-1} = y$. Hence we have $yx = xy$, and so G is abelian.

(ii) We prove it by induction on the order $n = |G|$. If $n = 1$, then $|G| = 2^0$. Let $n > 1$ and assume that the property holds true for every group of order smaller or equal to $n - 1$. Now let G be a finite group of order n satisfying the property, that is, every element of $G \setminus \{1\}$ has order 2. Let $x \in G \setminus \{1\}$. Then $ord(x) = 2$. We have the normal subgroup $N = < x > \trianglelefteq G$ and we may consider the factor group G/N. We have $|G/N| \leq n-1$. For every $g \in G \setminus \{1\}$, we have $ord(g) = 2$, and so $(gN)^2 = g^2N = N$. This shows that every element of $(G/N) \setminus \{N\}$ has order 2. By the induction hypothesis, we have $|G/ < x > | = 2^k$ for some $k \in \mathbb{N}^*$. But then we have $|G| = |G/ < x > | \cdot | < x > | = 2^k \cdot 2 = 2^{k+1}$.

Example 1.11.8 *Let us determine all (non-isomorphic) groups of order* 6.

Let $(G,\cdot)$ be a group of order 6.

Case I. If $(G,\cdot)$ has an element of order 6, then $(G,\cdot)$ is cyclic, and so $(G,\cdot)\cong(\mathbb{Z}_6,+)$.

Case II. Assume that G does not have elements of order 6. Then by Lagrange's Theorem, every element of $G\setminus\{1\}$ must have order 2 or 3. If every element of $G\setminus\{1\}$ has order 2, then the order of G must be a power of 2 by Example 1.11.7, contradiction. Hence $G\setminus\{1\}$ has an element a of order 3. Consider the cyclic subgroup $N=<a>=\{1,a,a^2\}$ of G. Since the index $|G:N|$ of N in G is $|G/N|=2$, we have $N\trianglelefteq G$ (see the course).

Let $b\in G\setminus N$. Since $|G:N|=2$, we must have $bN=Nb$, and so

$$\{b,ba,ba^2\}=\{b,ab,a^2b\}.$$

Note that $G/N=\{N,bN\}$, hence bN has order 2 in G/N, and so $b^2N=(bN)\cdot(bN)=N$. If $c\in bN$, then $c^3\in b^3N=bN$, and so $c^3N=bN$. This implies that $c^3\notin N$, hence $ord(c)=2$. Thus $ord(b)=ord(ba)=ord(ba^2)=2$.

So far, we have the following partial table operation on $G=N\cup bN=\{1,a,a^2,b,ba,ba^2\}$:

$\cdot$	1	a	a^2	b	ba	ba^2
1	1	a	a^2	b	ba	ba^2
a	a	a^2	1			
a^2	a^2	1	a			
b	b	ba	ba^2	1	a	a^2
ba	ba	ba^2	b		1	
ba^2	ba^2	b	ba			1

The equality $\{b,ba,ba^2\}=\{b,ab,a^2b\}$ implies that $ba=a^kb$ for some $k\in\{0,1,2\}$. Since $ord(ba)=ord(b)=2$, it follows that

$$1=(ba)\cdot(ba)=(a^kb)\cdot(ba)=a^{k+1},$$

whence $k=2$, because $ord(a)=3$. Hence $ba=a^2b$. Then the equality $\{b,ba,ba^2\}=\{b,ab,a^2b\}$ implies that $ab=ba^2$. Also taking into account that the table operation of a group G has the property that every element of G appears exactly once on each row and on each column we may finish to fill in uniquely the operation table of G as follows:

$\cdot$	1	a	a^2	b	ba	ba^2
1	1	a	a^2	b	ba	ba^2
a	a	a^2	1	ba^2	b	ba
a^2	a^2	1	a	ba	ba^2	b
b	b	ba	ba^2	1	a	a^2
ba	ba	ba^2	b	a^2	1	a
ba^2	ba^2	b	ba	a	a^2	1

A model for such a non-cyclic group of order 6 is the dihedral group $(D_3,\cdot)$. The roles of $a,b\in G$ are played by the rotation of 120^0 counterclockwise and one of the symmetries of an equilateral triangle respectively. Another model for it is the permutation group $(S_3,\circ)$.

In conclusion, for every group $(G,\cdot)$ of order 6, we have either $(G,\cdot)\cong(\mathbb{Z}_6,+)$ or $(G,\cdot)\cong(D_3,\cdot)$. Note that $(\mathbb{Z}_6,+)\ncong(D_3,\cdot)$ (one of them is cyclic and the other one is not).

Example 1.11.9 *Let us determine all (non-isomorphic) groups of order* 8.

Let $(G,\cdot)$ be a group of order 8.

Case I. If $(G,\cdot)$ has an element of order 8, then $(G,\cdot)$ is cyclic, and so $(G,\cdot)\cong(\mathbb{Z}_8,+)$.

Case II. Assume that G does not have elements of order 8. Then by Lagrange's Theorem, every element of $G\setminus\{1\}$ must have order 2 or 4. If every element of $G\setminus\{1\}$ has order 2, then G is abelian. A model for such a group is $(\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2,+)$.

In what follows, we assume that $G\setminus\{1\}$ has an element a of order 4. Consider the cyclic subgroup $N=<a>=\{1,a,a^2,a^3\}$ of G. Since the index $|G:N|$ of N in G is $|G/N|=2$, we have $N\trianglelefteq G$ (see the course).

Let $b \in G \setminus N$. Hence $ord(b) \in \{2,4\}$. Since $|G:N| = 2$, we must have $bN = Nb$, and so

$$\{b, ba, ba^2, ba^3\} = \{b, ab, a^2b, a^3b\}.$$

Note that $G/N = \{N, bN\}$, hence bN has order 2 in G/N, and so $b^2N = (bN)\cdot(bN) = N$. This implies that $b^2 \in N = \{1, a, a^2, a^3\}$. If $b^2 = a$, then $b^4 = a^2$, hence $ord(b) \notin \{2,4\}$, contradiction. If $b^2 = a^3$, then $b^4 = a^2$, hence $ord(b) \notin \{2,4\}$, contradiction. It follows that $b^2 \in \{1, a^2\}$.

So far, we have the following partial table operation on $G = N \cup bN = \{1, a, a^2, a^3, b, ba, ba^2, ba^3\}$:

$\cdot$	1	a	a^2	a^3	b	ba	ba^2	ba^3
1	1	a	a^2	a^3	b	ba	ba^2	ba^3
a	a	a^2	a^3	1				
a^2	a^2	a^3	1	a				
a^3	a^3	1	a	a^2				
b	b	ba	ba^2	ba^3				
ba	ba	ba^2	ba^3	b				
ba^2	ba^2	ba^3	b	ba				
ba^3	ba^3	b	ba	ba^2				

Case II (i). Assume that G is abelian. Hence $ab = ba$.

Now we have the following partial table operation on $G = N \cup bN = \{1, a, a^2, a^3, b, ba, ba^2, ba^3\}$:

$\cdot$	1	a	a^2	a^3	b	ba	ba^2	ba^3
1	1	a	a^2	a^3	b	ba	ba^2	ba^3
a	a	a^2	a^3	1	ba	ba^2	ba^3	b
a^2	a^2	a^3	1	a	ba^2	ba^3	b	ba
a^3	a^3	1	a	a^2	ba^3	b	ba	ba^2
b	b	ba	ba^2	ba^3				
ba	ba	ba^2	ba^3	b				
ba^2	ba^2	ba^3	b	ba				
ba^3	ba^3	b	ba	ba^2				

- If $b^2 = 1$, then $ord(b) = 2$ and we have the following table operation on G, whose missing part is computed by using the identities $ab = ba$ and $b^2 = 1$:

$\cdot$	1	a	a^2	a^3	b	ba	ba^2	ba^3
1	1	a	a^2	a^3	b	ba	ba^2	ba^3
a	a	a^2	a^3	1	ba	ba^2	ba^3	b
a^2	a^2	a^3	1	a	ba^2	ba^3	b	ba
a^3	a^3	1	a	a^2	ba^3	b	ba	ba^2
b	b	ba	ba^2	ba^3	1	a	a^2	a^3
ba	ba	ba^2	ba^3	b	a	a^2	a^3	1
ba^2	ba^2	ba^3	b	ba	a^2	a^3	1	a
ba^3	ba^3	b	ba	ba^2	a^3	1	a	a^2

  A model for such a group is $(\mathbb{Z}_4 \times \mathbb{Z}_2, +)$. The roles of $a, b \in G$ are played by $(1,0), (0,1) \in \mathbb{Z}_4 \times \mathbb{Z}_2$ respectively.

- If $b^2 = a^2$, then $ord(b) = 4$ and we have the following table operation on G, whose missing part is computed by using the identities $ab = ba$ and $b^4 = 1$:

$\cdot$	1	a	a^2	a^3	b	ba	ba^2	ba^3
1	1	a	a^2	a^3	b	ba	ba^2	ba^3
a	a	a^2	a^3	1	ba	ba^2	ba^3	b
a^2	a^2	a^3	1	a	ba^2	ba^3	b	ba
a^3	a^3	1	a	a^2	ba^3	b	ba	ba^2
b	b	ba	ba^2	ba^3	a^2	a^3	1	a
ba	ba	ba^2	ba^3	b	a^3	1	a	a^2
ba^2	ba^2	ba^3	b	ba	1	a	a^2	a^3
ba^3	ba^3	b	ba	ba^2	a	a^2	a^3	1

A model for such a group is again $(\mathbb{Z}_4 \times \mathbb{Z}_2, +)$. Note that if $c = ba$, then $c^2 = (ba)^2 = b^2a^2 = 1$, hence $ord(c) = 2$ and so $cN = bN$. Thus we are in the previous situation with b replaced by c.

Case II (ii). Assume that G is not abelian. Recall that we have the equality $\{b, ba, ba^2, ba^3\} = \{b, ab, a^2b, a^3b\}$. If $ab = ba^2$, then $a^2b = aba^2 = ba^4 = b$, contradiction. Hence we must have $ab = ba^3$.

Now we have the following partial table operation on G:

$\cdot$	1	a	a^2	a^3	b	ba	ba^2	ba^3
1	1	a	a^2	a^3	b	ba	ba^2	ba^3
a	a	a^2	a^3	1	ba^3	b	ba	ba^2
a^2	a^2	a^3	1	a	b	ba	ba^2	ba^3
a^3	a^3	1	a	a^2	ba	ba^2	ba^3	b
b	b	ba	ba^2	ba^3				
ba	ba	ba^2	ba^3	b				
ba^2	ba^2	ba^3	b	ba				
ba^3	ba^3	b	ba	ba^2				

- If $b^2 = 1$, then $ord(b) = 2$ and we have the following table operation on G, whose missing part is computed by using the identities $ab = ba^3$ and $b^2 = 1$:

$\cdot$	1	a	a^2	a^3	b	ba	ba^2	ba^3
1	1	a	a^2	a^3	b	ba	ba^2	ba^3
a	a	a^2	a^3	1	ba^3	b	ba	ba^2
a^2	a^2	a^3	1	a	b	ba	ba^2	ba^3
a^3	a^3	1	a	a^2	ba	ba^2	ba^3	b
b	b	ba	ba^2	ba^3	1	a	a^2	a^3
ba	ba	ba^2	ba^3	b	a^3	1	a	a^2
ba^2	ba^2	ba^3	b	ba	a^2	a^3	1	a
ba^3	ba^3	b	ba	ba^2	a	a^2	a^3	1

  A model for such a group is the dihedral group $(D_4, \cdot)$. The roles of $a, b \in G$ are played by the rotation of 90^0 counterclockwise and one of the symmetries of a square respectively.

- If $b^2 = a^2$, then $ord(b) = 4$ and we have the following table operation on G, whose missing part is computed by using the identities $ab = ba^3$ and $b^4 = 1$:

$\cdot$	1	a	a^2	a^3	b	ba	ba^2	ba^3
1	1	a	a^2	a^3	b	ba	ba^2	ba^3
a	a	a^2	a^3	1	ba^3	b	ba	ba^2
a^2	a^2	a^3	1	a	b	ba	ba^2	ba^3
a^3	a^3	1	a	a^2	ba	ba^2	ba^3	b
b	b	ba	ba^2	ba^3	a^2	a^3	1	a
ba	ba	ba^2	ba^3	b	a	a^2	a^3	1
ba^2	ba^2	ba^3	b	ba	1	a	a^2	a^3
ba^3	ba^3	b	ba	ba^2	a^3	1	a	a^2

  A model for such a group is the quaternion group $(Q, \cdot)$. The roles of $a, b \in G$ are played, for instance, by the elements i and j of Q.

In conclusion, every group $(G, \cdot)$ of order 8 is isomorphic to one of the following groups: $(\mathbb{Z}_8, +)$, $(\mathbb{Z}_4 \times \mathbb{Z}_2, +)$, $(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, +)$, $(D_4, \cdot)$ or $(Q, \cdot)$. Note that these groups are not isomorphic to each other, because they have different distributions of orders of elements (see Exercise 9 from Seminar 5).