Subgroups

Sergei Silvestrov

Spring term 2011, Lecture 9

Contents of the lecture

- Subgroups.
- Cyclic groups.
- Generating sets and Cayley digraphs.
Notation

Along with notation from previous lecture, other notations often used in algebra are:

<table>
<thead>
<tr>
<th>Notation in Lecture 8</th>
<th>Additive notation</th>
<th>Multiplicative notation</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a \ast b$</td>
<td>$a + b$</td>
<td>$ab$</td>
</tr>
<tr>
<td>$e$</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>$a'$</td>
<td>$-a$</td>
<td>$a^{-1}$</td>
</tr>
<tr>
<td>$a \ast a \ast \cdots \ast a$ (n times)</td>
<td>$na$</td>
<td>$a^n$</td>
</tr>
</tbody>
</table>

Additive notation is used only for abelian groups.

**Definition 1.** The **order** $|G|$ of a group $G$ is the cardinality of the set $G$. 
Subgroups

A subgroup $H$ of a group $G$ is a group contained in $G$ so that if $h, h' \in H$, then the product $hh'$ in $H$ is the same as the product $hh'$ in $G$. The formal definition of subgroup, however, is more convenient to use.

**Definition 2.** (Thm 7.10, Sec. 7.3, p. 182)
A subset $H$ of a group $G$ is a subgroup if

1. $1 \in H$;
2. If $a, b \in H$, then $ab \in H$;
3. if $a \in H$, then $a^{-1} \in H$.

**Theorem 1.** (Thm 7.11, Sec. 7.3, p. 182)
If $G$ is finite, then a non-empty $H \subset G$ is a subgroup if $a, b \in H \Rightarrow ab \in H$.

**Proof.** In finite $G$, for any $a \in G$ there exists positive integer $k$ such that $a^k = e$. Hence, for any $a \in H$,

$$a^{-1} = a^{k-1} \in H \text{ and } a^k = e \in H$$

because $a, b \in H \Rightarrow ab \in H$.

If $H$ is a subgroup of $G$, we write $H \leq G$; if $H$ is a proper subgroup of $G$, that is, $H \neq G$, then we write $H < G$. $G$ is the improper subgroup of $G$. The subgroup $\{1\}$ is the trivial subgroup of $G$. All other subgroups are nontrivial.

**Definition 3.** (Sec. 7.3, p. 183)
Center of $G$ is the subset in $G$ consisting of all elements which commute with every element in $G$:

$$Z(G) = \{a \in G \mid ag = ga \quad \forall g \in G\}$$

**OBS!** $G$ is abelian $\Leftrightarrow Z(G) = G$

**Theorem 2.** (Compare with Thm 7.12, Sec. 7.3, p. 183)
The center $Z(G)$ is abelian subgroup of $G$.

**Proof.** Do this as an exercise. For detailed proof see the end of p. 183 in the book. $\square$
Examples of subgroups

Example 1. For any \( n \in \mathbb{Z}^+ \), we have \((\mathbb{Z}_n, +) < (\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +) < (\mathbb{C}, +)\).

Example 2. Let \( \mathbb{C}^* = \mathbb{C} \setminus \{0\} \). Then, for any \( n \in \mathbb{Z}^+ \), we have \((U_n, \cdot) < (U, \cdot) < (\mathbb{C}^*, \cdot)\).

Example 3. The set of cardinality 4 may carry exactly two different group structures. The first is \((\mathbb{Z}_4, +)\),

\[
\begin{array}{c|cccc}
  +_4 & 0 & 1 & 2 & 3 \\
  \hline
  0 & 0 & 1 & 2 & 3 \\
  1 & 1 & 2 & 3 & 0 \\
  2 & 2 & 3 & 0 & 1 \\
  3 & 3 & 0 & 1 & 2 \\
\end{array}
\]

while the second is the Klein 4-group \( V \) (\( V \) abbreviates the original German term \( Vierergruppe \)):

\[
\begin{array}{c|cccc}
    & e & a & b & c \\
\hline
  e & e & a & b & c \\
  a & a & e & c & b \\
  b & b & c & e & a \\
  c & c & b & a & e \\
\end{array}
\]

\( \mathbb{Z}_4 \) has only one nontrivial proper subgroup \( \{0, 2\} \), while \( V \) has three nontrivial proper subgroups, \( \{e, a\} \), \( \{e, b\} \), and \( \{e, c\} \). This is shown at the following subgroup diagrams.

\[
\begin{array}{c|c|c|c|c}
  & \mathbb{Z}_4 & & & V \\
\hline
  & \{0, 2\} & & & \{e, a\} \\
\hline
  & \{0\} & & & \{e\} \\
\end{array}
\]
Extra info on **Klein four-group**
(See more in Wikipedia article **Klein four-group**)

The Klein four-group is the smallest non-cyclic group. The only other group with four elements, up to isomorphism, is \( \mathbb{Z}_4 \), the cyclic group of order four (see also the list of small groups).

All non-identity elements of the Klein group have order 2. It is abelian, and isomorphic to the dihedral group of order (cardinality) 4. It is also isomorphic to the direct sum \( \mathbb{Z}_2 \oplus \mathbb{Z}_2 \).

In 2D it is the symmetry group of a rhombus and of a rectangle which are not squares, the four elements being the identity, the vertical reflection, the horizontal reflection, and a 180 degree rotation.

In 3D there are three different symmetry groups which are algebraically the Klein four-group \( V \):

- one with three perpendicular 2-fold rotation axes: \( D_2 \)
- one with a 2-fold rotation axis, and a perpendicular plane of reflection: \( C_{2h} = D_{1d} \)
- one with a 2-fold rotation axis in a plane of reflection (and hence also in a perpendicular plane of reflection):

\[
C_{2v} = D_{1h}
\]

The three elements of order 2 in the Klein four-group are interchangeable: the automorphism group is the group of permutations of the three elements. This essential symmetry can also be seen by its permutation representation on 4 points:

\[
V = \{ \text{identity, } (1,2)(3,4), (1,3)(2,4), (1,4)(2,3) \}
\]

In this representation, \( V \) is a normal subgroup of the alternating group \( A_4 \) (and also the symmetric group \( S_4 \)) on 4 letters. In fact, it is the kernel of a surjective map from \( S_4 \) to \( S_3 \). According to Galois theory, the existence of the Klein four-group (and in particular, this representation of it) explains the existence of the formula for calculating the roots of quartic equations in terms of radicals, as established by Lodovico Ferrari: the map corresponds to the resolvent cubic, in terms of Lagrange resolvents.

Another example of the Klein four-group is the multiplicative group \( \{1,3,5,7\} \) with the action being multiplication modulo 8.

In the construction of finite rings, eight of the eleven rings with four elements have the Klein four-group as their additive substructure.
Cyclic subgroups

**Definition 4.** (Sec. 7.3, p. 84)
If $G$ is a group and $a \in G$, write
\[
\langle a \rangle = \{ a^n : n \in \mathbb{Z} \}.
\]
$\langle a \rangle$ is called the **cyclic subgroup** of $G$ **generated** by $a$. A group $G$ is called **cyclic** if there exists $a \in G$ with $G = \langle a \rangle$, in which case $a$ is called a **generator** for $G$.

**Obs!** The fact that $\langle a \rangle$ is a subgroup of $G$ is an easy exercise stated as **Theorem 7.13.** on page 184 in the book.

**Can you prove it yourself NOW in 3 minutes?**

**Example 4.** For any $n \in \mathbb{Z}^+$, $U_n$ is a cyclic group with $\zeta = e^{2\pi i / n}$ as a generator, i.e., $U_n = \langle 1 \rangle$.

Because $\mathbb{Z}_n$ is isomorphic to $U_n$, $\mathbb{Z}_n$ is also a cyclic group with 1 as a generator, i.e., $\mathbb{Z}_n = \langle 1 \rangle$.

Check that $\mathbb{Z}_4 = \langle 3 \rangle$.

**Example 5.** $V$ is **not** cyclic, because $\langle a \rangle$, $\langle b \rangle$, and $\langle c \rangle$ are proper subgroups.

**Example 6.** $(\mathbb{Z}, +) = \langle 1 \rangle$. For any $n \in \mathbb{Z}$, the cyclic subgroup generated by $n$, $\langle n \rangle$, consists of all multiples of $n$, and is denoted by $n\mathbb{Z}$. We have $n\mathbb{Z} = -n\mathbb{Z}$. 
Properties of cyclic groups

Let $G$ be a group, and let $a \in G$. If $\langle a \rangle$ is finite, then the order of $a$ is the order $|\langle a \rangle|$ of this cyclic subgroup. Otherwise, we say that $a$ is of infinite order.

Theorem 3. Every cyclic group is abelian.

Theorem 4. (Thm 7.16, Sec. 7.3, p. 185)
Any subgroup $H$ of a cyclic group $G = \langle a \rangle$ is cyclic (and more precisely $H = \langle a^k \rangle$ where $k = \min \{k > 0 \mid a^k \in H\}$)

Proof. Let $k = \min \{k > 0 \mid a^k \in H\}$. Any $m$ such that $a^m \in H$ can be written by division algorithm in $\mathbb{Z}$ as $m = qk + r, \ 0 \leq r < k$. Thus $r = m - kq$ and hence $a^r = a^m(a^k)^{-q} \in H$ and therefore $r = 0$ by choice of $k$ as minimal. So, $a^m = (a^k)^q \in \langle a^k \rangle$ and hence $H = \langle a^k \rangle$. \qed

Corollary 1. The subgroups of $(\mathbb{Z}, +)$ are $(n\mathbb{Z}, +)$ for $n \in \mathbb{Z}$. 
The structure and generators of cyclic groups and subgroups

**Theorem 5** (The structure of cyclic groups, Thm 7.18, Sec. 7.4, p. 193). Every infinite cyclic group is isomorphic to the group \((\mathbb{Z}, +)\) and every finite cycle group of order \(m\) is isomorphic to the group \((\mathbb{Z}_m, +_m)\).

**Proof.** If \(G = \langle a \rangle\) is a cyclic group, then \(f(k) = a^k\) defines isomorphism in both cases. For more details see p. 193 in the book.

Let \(r \in \mathbb{Z}^+\) and \(s \in \mathbb{Z}^+\). Let \(H = \langle r, s \rangle\) denotes the smallest subgroup in \((\mathbb{Z}, +)\) containing both \(r\) and \(s\). \(H\) is a subgroup of \((\mathbb{Z}, +)\). One can prove that \(H = \{ nr + ms : n, m \in \mathbb{Z}^+ \}\). By Corollary 1, \(H\) has a generator \(d \in \mathbb{Z} \setminus \{0\}\), that can be chosen to be positive.

**Definition 6.** The positive generator \(d\) of the cyclic group \(H = \{ nr + ms : n, m \in \mathbb{Z}^+ \}\) is called the greatest common divisor of \(r\) and \(s\).

**Definition 7.** Two positive integers \(r\) and \(s\) are relatively prime if their greatest common divisor is 1.

**Theorem 6.** Let \(G = \langle a \rangle\) and \(|G| = n\). Let \(b = a^r \in G\). Let \(d\) be the greatest common divisor of \(n\) and \(s\), and let \(H = \langle b \rangle\). Then \(|H| = n/d\). In particular, \(b\) generates all of \(G\) if and only if \(r\) is relatively prime with \(n\).

**Example 7.** The following subgroup diagram is obtained from Theorem 6 by direct calculations.

\[
\begin{align*}
\langle 1 \rangle &= \mathbb{Z}_{18} \\
\langle 2 \rangle &= \mathbb{Z}_9 & \langle 3 \rangle &= \mathbb{Z}_6 \\
\langle 6 \rangle &= \mathbb{Z}_3 & \langle 9 \rangle &= \mathbb{Z}_2 \\
\langle 0 \rangle &= \mathbb{Z}_1
\end{align*}
\]
Generating sets

Let \((G, \cdot)\) be a group, and let \(S\) be a subset of \(G\).

**Theorem 7.** Let \(\langle S \rangle\) be the set of elements of \(G\) consisting of all products \(x_1 \ldots x_n\) such that \(x_i\) or \(x_i^{-1}\) is an element of \(S\) for each \(i\), and also containing the unit element. It is the smallest subgroup of \(G\) containing \(S\).

**Definition 8.** The elements of \(S\) are called the *generators* of \(\langle S \rangle\). If \(\langle S \rangle = G\), we say that \(S\) generates \(G\). If there exists a finite set \(S\) that generates \(G\), then \(G\) is *finitely generated*.

**Example 8.** \((\mathbb{Z}, +) = \langle 1 \rangle\) is a finitely generated group. Its subgroup \(\langle r, s \rangle\) is also generated by one element \(d\), which is the greatest common divisor of \(r\) and \(s\).
Directed graphs: definition

Definition 9. A directed graph (or just digraph) is a finite set of points called vertices and some arcs (with a direction denoted by an arrowhead or without a direction) joining vertices.

For each generating set $S$ of a finite group $G$, we can construct the following Cayley digraph $D$. The number of vertices in $D$ is $|G|$. For any $a \in S$, there exist arcs of type $a$. An arc of type $a$ points from $x \in G$ to $y \in G$ if and only if $y = xa$. If $a \in S$ and $a^2 = e$, it is customary to omit the arrowhead from the arc of type $a$.

Example: Cayley digraph for $G = \mathbb{Z}_6$ and $S = \{1\}$

Example 9. Let $G = \mathbb{Z}_6$ and $S = \{1\}$. The Cayley digraph has the form

```
0 → 5 → 1
↑   ↑   ↓
4 → 2 → 3
```

– Typeset by Foil\TeX –
Example: Cayley digraph for $G = \mathbb{Z}_6$ and $S = \{2, 3\}$

**Example 10.** Let $G = \mathbb{Z}_6$ and $S = \{2, 3\}$. Let $\rightarrow$ be an arrow of type 2. Because $3^2 = 0$ in $\mathbb{Z}_6$, the arrow of type 3 must be $\rightarrow$. The Cayley digraph has the form

![Cayley digraph diagram](image-url)
A characterisation of Cayley digraphs

**Theorem 8.** A digraph $\mathcal{G}$ is a Cayley digraph of some generating set $H$ of a finite group $G$ if and only if the following four properties are satisfied.

1. $\mathcal{G}$ is connected.
2. At most one arc goes from vertex $g$ to a vertex $h$.
3. Each vertex $g$ has exactly one arc of each type starting at $g$, and one of each type ending at $g$.
4. If two different sequences of arc types starting from vertex $g$ lead to the same vertex $h$, then those same sequences of arc types starting from any vertex $u$ will lead to the same vertex $v$.

Cayley used this theorem to construct new groups. For example, the following digraph satisfies all conditions of Theorem 8.

If we label $\longrightarrow$ by $a$ and $\quad \dashrightarrow$ by $b$, we obtain a Cayley digraph of a new group of order $8$: