Abstract Algebra, Lecture 4

Cyclic Groups

Jan Snellman[1]

[1]Matematiska Institutionen
Linköpings Universitet

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Summary

Summary

Summary

Summary

Group

Recall:

Definition

$(G, *, 1)$ is a group if for all $a, b, c \in G$,

1. $a * (b * c) = (a * b) * c$,
2. $a * 1 = e * 1 = a$,
3. exists unique $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = 1$.

If $a * b = b * a$ always, then abelian group.

Remember: in $\mathbb{Z}_n$, $g = [a]_n$ has multiplicative inverse iff $\gcd(a, n) = 1$.

Definition

$\mathbb{Z} \ni n > 1$.

- $U_n = \{ [a]_n | \gcd(a, n) = 1 \}$.
- $\phi(n) = |\{ 1 \leq a < n | \gcd(a, n) = 1 \}| = |U_n|$.

Example

$U_5 = \{[1]_5, [2]_5, [3]_5, [4]_5\}$, $U_6 = \{[1]_6, [5]_6\}$.

Example

Multiplication in U_5 and U_8

*	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

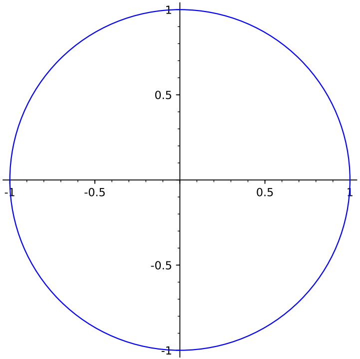
*	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Definition

The punktured complex plane $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ is an abelian group under complex multiplication. The circle group

$$\mathfrak{T} = \{ z \in \mathbb{C}^* \,|\, |z| = 1 \}$$

forms a subgroup.



Definition

- G group, $g \in G$.
- $g^0 = 1$.
- $g^2 = g * g$, $g^3 = g * g * g$, et cetera; for n positive integer g^n is g times itself n times (associativity makes this unambiguous)
- $g^{-2} = g^{-1} * g^{-1} = (g * g)^{-1}$; $g^{-n} = (g^n)^{-1} = (g^{-1})^n$.

Lemma

For all $g \in G$, $i, j \in \mathbb{Z}$, it holds that

$$g^i * g^j = g^{i+j}.$$

Definition

The element $g \in G$ has order n, written $o(g) = n$, if

$$g^n = 1$$

but

$$g^m \neq 1 \quad \text{for} \quad 1 \leq m < n.$$

If $g^n \neq 1$ for all $n > 0$ then the order of g is infinite. It is understood that the unit element has order one.

Example

- $3^2 = 9 \equiv 1 \mod 8$, so $[3]_8$ has order 2 as an element in U_8.
- $3^2 = 9 \equiv 4 \mod 5$, $3^3 = 27 \equiv 2 \mod 5$, $83^4 = 81 \equiv 1 \mod 5$, so $[3]_5$ has order 4 as an element of U_5.
- $5 \in \mathbb{Z}$ has infinite order

Definition

$g \in G$, G group. We define the cyclic subgroup generated by g as

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

Lemma

This is the smallest subgroup of G that contain g; it can be written

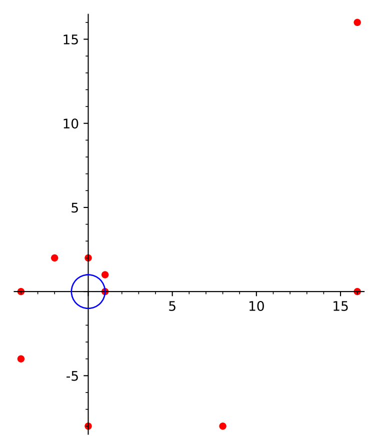
$$\langle g \rangle = \bigcap_{g \in H \leq G} H$$

Lemma

$o(g) = |\langle g \rangle|$

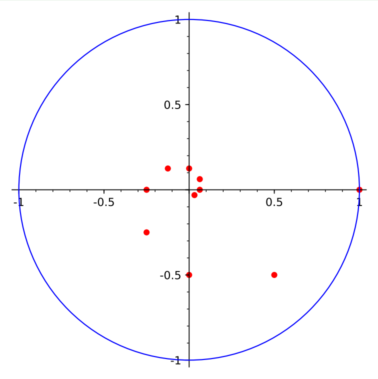
Example

$G = \mathbb{C}^*$, $g = 1 + i$. We depict $g^0, g, g^2, g^3, \ldots, g^9$:



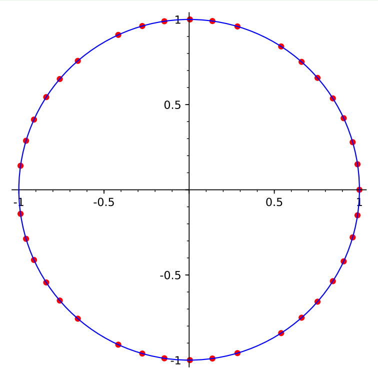
Example

$G = \mathbb{C}^*$, $g = 1 + i$. We depict $g^0, g^{-1}, g^{-2}, g^{-3}, \ldots, g^{-9}$:



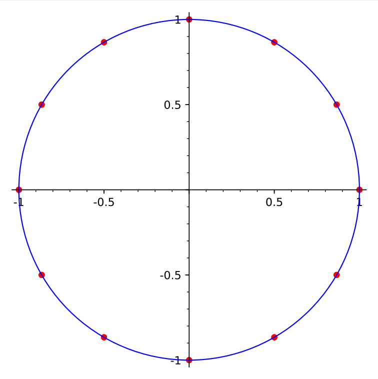
Example

$h = e^i \in \mathfrak{T}$. We depict $g^{-9}, \ldots, g^9$:



Example

$w = e^{\pi i/6} \in \mathfrak{T}$. We depict $g^{-9}, \ldots, g^{9}$:



Definition

A group G is cyclic if it has a generator g, i.e., an element such that $G = \langle g \rangle$.

Example

- $\mathbb{C}^*$ is not cyclic
- $\mathfrak{T}$ is not cyclic
- $\langle e^i \rangle$ is cyclic, and infinite
- $\langle i \rangle$ is cyclic, and finite

Definition

If G is abelian, the operation is often denoted $+$, and the identity element 0. Then for $g \in G$,

- $ng = g + \cdots + g$ if $n > 0$
- $0g = 0$,
- $(-n)g = -(ng) = -g - g \cdots - g$
- $\langle g \rangle = \mathbb{Z}g = \{ ng | n \in \mathbb{Z} \}$

Theorem

- *$\mathbb{Z}$ is an infinite cyclic group, generated by 1, or by -1.*
- *For any $n \geq 2$, $\mathbb{Z}_n$ is finite cyclic group, generated by $[1]_n$, and by any $[a]_n \in U_n$.*

Proof.

First part: obvious.

Second part: $xa = a + \cdots + a$, sum of a x times. We can solve

$$xa \equiv b \mod n$$

for all RHS b iff $\gcd(a, n) = 1$. $\square$

Definition

An *isomorphism* between groups G, H is a bijection $\phi : G \to H$ satisfying, for all $x, y \in G$,

$$\phi(x *_G y) = \phi(x) *_H \phi(y)$$

If an isomorphism exists between G and H, the groups are said to be isomorphic.

Isomorphic groups are, from a group-theoretic point of view, the same. The multiplication is the same, after a relabeling of the elements, provided by ϕ. Isomorphic groups have the same properties (beeing abelian, cyclic, et cetera) and have of course the same size.

Example

Consider the following four matrices, corresponding to reflections in the coordinate axes in the plane:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad T = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad R = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

(well, the last one is a rotation by halv a turn). They form a group, with multiplication table

*	I	S	T	R
I	I	S	T	R
S	S	I	R	T
T	T	R	I	S
R	R	T	S	I

Example (Cont)

Now consider the invertible maps on $\{1, 2, 3, 4\}$ given by

1. The identity
2. Swapping 2 and 4
3. Swapping 1 and 3
4. Swapping 1 and 3, and simultaneously 2 and 4

Call the maps i, a, b, c. They form a group unto themselves! The multiplication table is

*	i	a	b	c
i	i	a	b	c
a	a	i	c	b
b	b	c	i	a
c	c	b	a	i

Example (Cont)

Now place the multiplication tables side-by-side:

*	I	S	T	R
I	I	S	T	R
S	S	I	R	T
T	T	R	I	S
R	R	T	S	I

*	i	a	b	c
i	i	a	b	c
a	a	i	c	b
b	b	c	i	a
c	c	b	a	i

We see that the relabeling

$$I \to i$$
$$S \to a$$
$$T \to b$$
$$R \to c$$

turns one table into the other, proving that the groups are isomorphic.

Theorem

Let $G = \langle g \rangle$ be a cyclic group. If G is infinite, then it is isomorphic to $\mathbb{Z}$. If it has finite order n, then it is isomorphic to $\mathbb{Z}_n$.

Proof

- $G = \langle g \rangle = \{ g^n | n \in Z \}$
- Case 1: all g^n are different. Exponent laws: $g^n * g^m = g^{n+m}$, bijection to $\mathbb{Z}$ which preserves multiplication.
- Case 2: exists some smallest $0 < m < n$ such that $g^m = g^n$ (i.e. m smallest, then n smallest for that m)
- Multiply by g^{-m}, get $1 = g^0 = g^{n-m}$, put $k = n - m$. Smallest positive k such that $g^k = 1$.
- $(g^k)^s = 1 = g^{ks}$, thus $g^t = 1$ whenever $k|t$. If divides not, write $t = kt + r$, then $g^t = g^{kt} g^r = g^r \neq 1$ since $1 < r < k$, and k smallest.

Proof.

Proof, cont

- Get that $g^a = g^b$ if and only if $a \equiv b \mod n$
- Thus $[a]_n \mapsto g^a$ well-defined bijection, and isomorphism by exponent laws.

$\square$

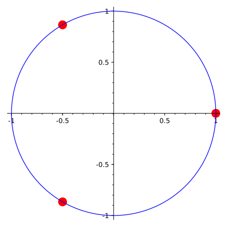
For convenience (to avoid additive notation, and to avoid tying the abstract notion to the concrete integers) we introduce

Definition

The infinite cyclic (multiplicative) group is denoted C_∞, and the cyclic group of order n is denoted C_n.

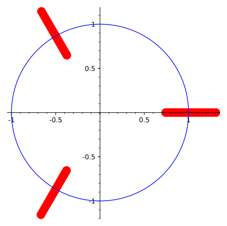
Example

These cyclic groups are all isomorphic to C_3:

1. $\mathbb{Z}_3$,
2. $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$, and $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$
3. 

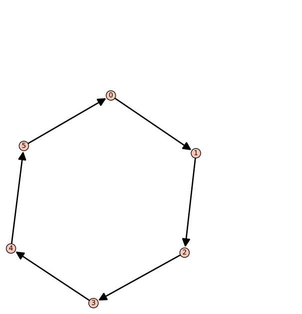
Example

These cyclic groups are all isomorphic to C_∞:

1. $\mathbb{Z}$,
2. $\left\langle \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix} \right\rangle$
3. 

Example

If A is an invertible matrix, then since it is an element of a group, its positive powers $A, A^2, A^3, \ldots$ are either all different, or there is an n such that $A^n = I$ and the higher powers repeat, according to $A^{nk+r} = A^r$. For instance, if $n = 6$, we can depict the situation as follows:



The sequence of powers of A is purely periodic, with period 6:

$$A^0 = I, A^1, A^2, A^3, A^4, A^5, A^6 = I, A^7 = A^1, \ldots$$

Example (Cont)

Compare what happens when we are in a semigroup: let

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

This is a non-invertible matrix, hence we are in the semigroup of (not necessarily invertible) 4x4 matrices. Let us compute its first 5 powers:

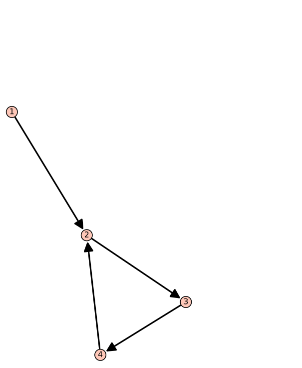
$$\left[\begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} \right]$$

So the sequence repeats after a pre-period:

$$A^1, A^2, A^3, A^4, A^5 = A^2, A^6 = A^3, \ldots$$

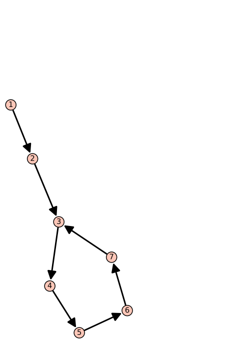
Example (Cont)

A picture of the powers of A is now like this:



Example (Cont)

The non-invertible map from $\{1, 2, \ldots, n+m\}$ which sends i to $i+1$ for $1 \leq i \leq n+m-1$, and $n+m$ to $m+1$, has pre-period m and period n. Here is a picture of $m = 3$ and $n = 4$:



Theorem

The subgroups of the cyclic group $G = \langle g \rangle$ are all cyclic, given by $H = \langle g^k \rangle$. If G is infinite, all subgroups except $\langle g^0 \rangle = \{1\}$ are infinite (hence isomorphic to G itself.)
If $|G| = n$, then $H = G$ whenever $\gcd(k, n) = 1$; otherwise, $|H| = \frac{n}{\gcd(k,n)}$.

Proof.

First assertion: obvious. Second assertion: we prove that in any group, if $o(g) = n < \infty$, then $o(g^k) = \frac{n}{\gcd(n,k)}$. Put $d = \gcd(n, k)$. Then $(g^k)^t = g^{kt} = 1$ iff $kt \equiv 0 \mod n$, which happens iff $\frac{k}{d}t \equiv 0 \mod \frac{n}{d}$. But $\gcd(\frac{k}{d}, \frac{n}{d}) = 1$, so this happens iff $t \equiv 0 \mod \frac{n}{d}$. $\square$

To describe the inclusions among the subgroups of a cyclic group, we use additive notations:

Theorem

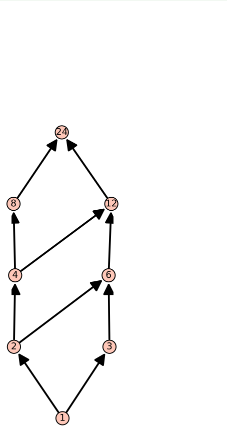
- *The subgroup $n\mathbb{Z}$ of $\mathbb{Z}$ is a subgroup of $m\mathbb{Z}$ if and only if $m|n$*
- *The subgroups of $\mathbb{Z}_n$ are $d\mathbb{Z}_n$ for $d|n$; furthermore $d_1\mathbb{Z}_n \leq d_2\mathbb{Z}_n$ if and only if $d_2|d_1$.*

Proof.

Try to prove it yourself! $\square$

Example

The subgroups of $C_{24} = \langle g \rangle$ are given by $\langle g^1 \rangle$, $\langle g^2 \rangle$, $\langle g^3 \rangle$, $\langle g^4 \rangle$, $\langle g^6 \rangle$, $\langle g^8 \rangle$, $\langle g^{12} \rangle$, $\langle g^{24} \rangle$, where $\langle g^1 \rangle$ is the largest, and $\langle g^{24} \rangle = \langle g^0 \rangle$ the smallest. Compare with the divisor lattice of 24:



Definition

G group, $S \subseteq S$ a subset. We define $\langle S \rangle$ as the smallest subgroup of G that contains S, i.e., as

$$\langle S \rangle = \bigcap_{S \subseteq H \leq G} H$$

If $S = \{a, b\}$, then

$$\langle S \rangle = 1, a, b, a^{-1}, b^{-1}, a^2, ab, ba, b^2, ab^{-1}, \ldots, ab^{-1}ab^2a^{-2}, \ldots$$

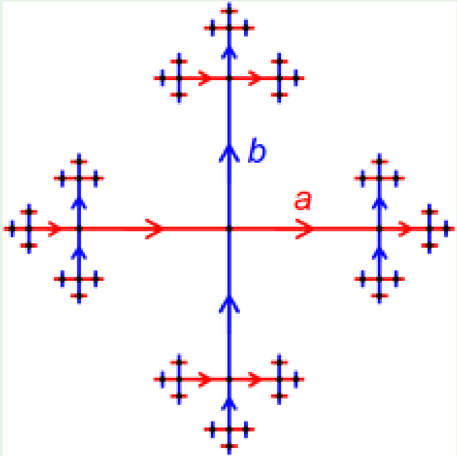
i.e., it consists of all words

$$z_1 * z_2 * \cdots * z_N, \qquad z_i \in \left\{a, b, a^{-1}, b^{-1}\right\}$$

which are reduced, so a, a^{-1} are not adjacent, neither is b, b^{-1}.

Example

If there are no further relations between a and b, i.e, if the reduced words represent distinct group elements, then we get the *free group* on two generators. It can be depicted graphically as follows:

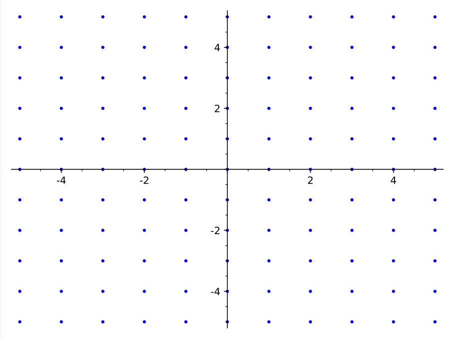


Example

If we instead impose the commutativity relation $ab = ba$, then the set of elements reduce to

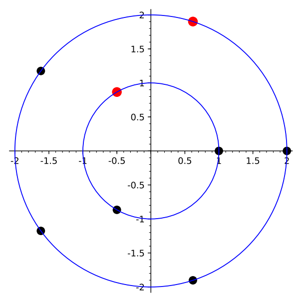
$$a^m b^n, \qquad n, m \in \mathbb{Z}$$

This group, which is generated by a and b together, can be depicted as



Example

If we impose $ab = ba$, $a^3 = 1$, $b^5 = 1$, the resulting group is the set of all $a^n b^m$, where n is to be taken modulo 3, and m is to be taken modulo 5. The elements can be thought of as a pair of points on two concentric circles:



Definition

Let G, H be groups. Their direct product $G \times H$ has the cartesian products of their underlying sets as its underlying set, and operation derived from those on G and on H.

$$(g_1, h_1) * (g_2, h_2) = (g_1 *_G g_2, h_1 *_H h_2)$$

The identity element is

$$(1_G, 1_H)$$

and the inverse is given by

$$(g, h)^{-1} = (g^{-1}, h^{-1})$$

Definition

For three groups G, H, K, we have natural isomorphism

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

so we can denote this product simply by $G \times H \times K$. The direct product $G \times G$ is denoted G^2, $G \times G \times G = G^3$, and so on.

Note: it is also true that $G \times H \simeq H \times G$.

Theorem

If $g \in G$, $o(g) = m < \infty$, $h \in H$, $o(h) = n < \infty$, then the order of $(g, h) \in G \times H$ is $lcm(m, n)$

Proof.

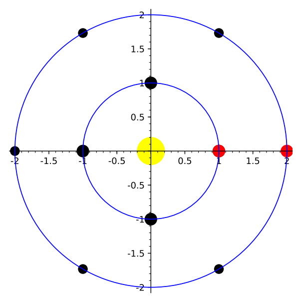
We have that $(g, h)^s = (1, 1)$ if and only iff $g^s = !_G$ and $h^s = 1_H$, which happens if and only if

$$s \equiv 0 \mod m$$
$$s \equiv 0 \mod n$$

which in turns happens if and only if $\mathrm{lcm}(m, n) | s$. $\square$

Example

If the planet Mars takes 4 (Terran) years to make a revolution around the Sun, and the tiny asteroid "Pluttinutt" takes 6 years, then the constellations of the Sol-Mars-Pluttinutt system repeat with a period of $\mathrm{lcm}(4,6) = 12$ years.



Theorem

Let m, n be positive integers. Then $C_m \times C_n$ is cyclic if and only if $\gcd(m, n) = 1$.

Proof

Let g and h be generators of C_m and C_n, respectively. Put $\tilde{g} = (g, 1)$, and $\tilde{h} = (1, h)$. Then

$$o((g, h) = o(\tilde{g}\tilde{h}) = \mathrm{lcm}(m, n) = \frac{mn}{\gcd(m, n)},$$

so if $\gcd(m, n) = 1$, then

$$\tilde{g}\tilde{h} = mn = |C_m||C_n| = |C_m \times C_n|$$

so $C_m \times C_n$ is cyclic.

Proof, contd.

On the other hand, suppose that $C_m \times C_n$ is cyclic, with generator (x, y). Then $o((x, y)) = mn = \mathrm{lcm}(o(x), o(y))$. Since the maximal order of an element in C_m is m, and the maximal order of an element in C_n is n, it follows that $o(x) = m$ and $o(y) = n$ and $\mathrm{lcm}(m, n) = mn$. $\square$

Example

$C_3 \times C_5 \simeq C_{15}$. On the other hand, $C_2 \times C_2$ is not cyclic, since all non-indentity elements have order 2. We re-use one of the groups we studied before, with multiplication table

*	I	S	T	R
I	I	S	T	R
S	S	I	R	T
T	T	R	I	S
R	R	T	S	I

This group is isomorphic to the direct product

$$\{I, S\} \times \{I, T\}$$

where each factor is isomorphic to C_2. Note that the square of each element is the identity, so elements have order one or two.