



KTH Teknikvetenskap

**SF2729 GROUPS AND RINGS
LECTURE NOTES
2010-02-02**

MATS BOIJ

2. THE SECOND LECTURE - SUBGROUPS, CYCLIC GROUPS AND CAYLEY DIGRAPHS

The second lecture introduces subgroups and, deals with cyclic groups, generators of groups and Cayley digraphs.¹

Definition 2.1 (Subgroup). We say that a group H which is a non-empty subset of a group G is a *subgroup* of G , denoted by $H \leq G$ if the binary operation on H is the restriction of the binary operation on G , i.e., if H is a group with the same group operation.

Example 2.2.

- (1) The set of even integers $2\mathbb{Z}$ form a subgroup of the integers, \mathbb{Z} under addition.
- (2) More generally, for any integer n we have that $n\mathbb{Z} \leq \mathbb{Z}$.
- (3) The trivial subgroup $\{e\}$ is a subgroup in any group, $\{e\} \leq G$.
- (4) The group itself is a subgroup, $G \leq G$.

Definition 2.3 (non-trivial, proper). A subgroup $H \leq G$ is *non-trivial* if $H \neq \{e\}$. It is *proper* if $H \neq G$ and in this case we write $H < G$.

It is convenient to notice that we can check whether a subset of a group forms a subgroup by the following result:

Theorem 2.4. *Let H be a non-empty subset of a group G . Then H is a subgroup of G if and only if*

- i) H is closed under the group operation, i.e., $a, b \in H \implies a * b \in H$*
- ii) H is closed under taking inverses, i.e., $a \in H \implies a^{-1} \in H$*

Proof. If H is a subgroup, then the group operation on G defines the group operation on H and hence H must be closed under this operation and under taking inverses.

Suppose that H satisfies the two conditions. Now $*$ defines a binary operation on H , which has to be associative, since it is associative on a larger set G . The unit of G has to be in H since $a \in H \implies a^{-1} \in H \implies e = aa^{-1} \in H$. Hence the three axioms for a group holds for the restriction of the group operation on G to the subset H . \square

¹The second lecture is based on the sections 5-7 of Chapter I in A First Course in Abstract Algebra [1].

Example 2.5. We can now easily get many more examples of subgroups:

- (1) The set of matrices of determinant one, $\text{Sl}_n(\mathbb{R}) \leq \text{Gl}_n(\mathbb{R})$ - the *special linear group*.
- (2) The set of orthogonal matrices, $\text{O}_n(\mathbb{R}) \leq \text{Gl}_n(\mathbb{R})$ — the *orthogonal group*.
- (3) The set of even permutations $A_n \leq S_n$ — the *alternating group*.

Corollary 2.6. *If H is a finite subset of a group G , then H is a subgroup if it is closed under the group operation.*

Corollary 2.7. *Let g be any element of H . If H is finite and closed under the group operation, some powers of g have to be equal, say $g^i = g^j$, $i < j$. By cancellation in G , we get $g^{j-i} = e$. Hence $g^{-1} = g^{j-i-1} \in H$ and H is closed under taking inverses.*

Definition 2.8 (Order and cyclic subgroups). Any element g of a groups G generates a subgroup, $\langle g \rangle = \{g^i | i \in \mathbb{Z}\}$. This is the *cyclic subgroup generated by g* . The *order* of a group is its cardinality, i.e., the number of elements and the *order of an element g* is the order of the cyclic subgroup generated by g .

Remark 2.9. We have to check that $\langle g \rangle$ really is a subgroup, which is easily done by verifying that

- $g^i * g^j = g^{i+j} \in \langle g \rangle$
- $g^{-1} \in \langle g \rangle$ since $-1 \in \mathbb{Z}$.

Another important way to get subgroups of a group is from maps between groups.

Definition 2.10 (homomorphism, isomorphism, kernel, image). A map $\phi : G \longrightarrow H$ between groups is a *group homomorphism* if it respects the group structure, i.e., if

$$\phi(g_1 * g_2) = \phi(g_1) * \phi(g_2), \quad \forall g_1, g_2 \in G.$$

A *group isomorphism* is a bijective group homomorphism, and if $\phi : G \longrightarrow H$ is an isomorphism, we say that G and H are isomorphic. The *kernel* of ϕ is given by

$$\ker \phi = \{g \in G | \phi(g) = e\}$$

and the *image* of ϕ is given by

$$\text{im} \phi = \{\phi(g) | g \in G\}.$$

Exercise 2.11. *Prove that the kernel and image of a group homomorphism $\phi : G \longrightarrow H$ are subgroups, i.e., that $\ker \phi \leq G$ and $\text{im} \phi \leq H$.*

Exercise 2.12. *Prove that $\phi^{-1}(K) \leq G$ if $\phi : G \longrightarrow H$ is a group homomorphism and $K \leq H$.*

Example 2.13. The subgroups $A_n \leq S_n$ and $\text{Sl}_n(\mathbb{R}) \leq \text{Gl}_n(\mathbb{R})$ are kernels of the homomorphisms:

$$\text{sgn} : S_n \longrightarrow \{\pm 1\} \quad \text{and} \quad \det : \text{Gl}_n \longrightarrow \mathbb{R}^*.$$

Exercise 2.14. *Prove that a group homomorphism is injective if and only if the kernel is trivial.*

2.1. Cyclic groups.

Definition 2.15 (Cyclic group). A group G is *cyclic* if there is an element $g \in G$ such that $G = \langle g \rangle$. Such an element is called a *generator* of G .

Theorem 2.16. A cyclic group is either infinite, and isomorphic to \mathbb{Z} under addition, or finite and isomorphic to \mathbb{Z}_n under addition for some positive integer n .

Proof. If g is a generator and G , we get a surjective homomorphism from $\phi : \mathbb{Z} \longrightarrow G$ by $\phi(i) = g^i$.

If the kernel of ϕ is trivial, ϕ is an isomorphism and G is infinite.

If there is a non-trivial kernel of this homomorphism, let n be the smallest positive integer in $\ker \phi$. Then we have that $g^n = e$, but $g^i \neq e$ for $0 < i < n$. Hence ϕ induces an isomorphism $\bar{\phi} : \mathbb{Z}_n \longrightarrow G$, by $\bar{\phi}([i]) = g^i$. This is well-defined since

$$[i] = [j] \iff j = kn + i \implies g^j = g^{kn+i} = e^k g^i = g^i.$$

□

Theorem 2.17. A subgroup of a cyclic group is cyclic.

Proof. According Theorem 2.16, it is enough to prove the statement for \mathbb{Z} and for \mathbb{Z}_n under addition.

If $H \leq \mathbb{Z}$ is a subgroup, we can let d be the smallest positive integer in H . Now $\langle d \rangle \leq H$. If n is any integer in H , we can write $n = qd + r$, where $0 \leq r < d$. Since H is a subgroup, $r = n - qd$ is in H since n and d are in H . Hence $r = 0$ by the assumption on d and $n = qd \in \langle d \rangle$.

Let $H \leq \mathbb{Z}_n$ be a subgroup. Then $\phi^{-1}(H) = \{i \in \mathbb{Z} \mid \phi(i) \in H\}$ is a subgroup of \mathbb{Z} , where $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ is the natural surjective homomorphism given by $\phi(i) = [i]$. By the above argument we can find $d \in \mathbb{Z}$ such that $\langle d \rangle = \phi^{-1}(H)$. This means that every element in H can be written as $\phi(nd)$ for some n , but this means that $H = \langle \phi(d) \rangle$ and H is cyclic. □

Theorem 2.18. Let G be a cyclic group of order n . Then G has a unique subgroup of order d for any positive divisor d in n .

Proof. We may identify G with \mathbb{Z}_n under addition. For any divisor d in n , we may take the subgroup $\langle [n/d] \rangle$. This subgroup has order d since $[n/d]$ has order d .

If H is a subgroup of order d , let m be the least positive integer such that $[m] \in H$. Then H is generated by m as we saw earlier. Now, $[m]$ has to have order d , which implies that in fact $m = n/d$. □

2.2. Generating sets and Cayley digraphs.

Definition 2.19 (Subgroup generated by a set). If S is a subset of a group G , we let $\langle S \rangle$ denote the *subgroup generated by S* , i.e., the intersection of all subgroups of G that contain S .

Remark 2.20. We should check that the definition makes sense by checking that $\langle S \rangle$ is in fact a subgroup. There is at least one subgroup that contains S , namely G itself. The intersection of any set of subgroups is again a subgroup, since

$$g, h \in \bigcap_{i \in I} H_i \implies g, h \in H_i, \forall i \in I \implies g * h \in H_i, \forall i \in I \implies g * h \in \bigcap_{i \in I} H_i.$$

and similarly for the inverses.

Theorem 2.21. We have that $\langle S \rangle = \{a_1 a_2 \cdots a_n \mid a_i \in S \text{ or } a_i^{-1} \in S, \text{ for some } n\}$.

Proof. All the element in the right hand side has to be in any subgroup that contains S , since any subgroup is closed under the group operation and under taking inverses. Thus is is sufficient to prove that the right hand side is in fact a subgroup.

It is closed under the group operation since we can compose two such expressions to a longer expression, and it is closed under inverses since

$$(a_1 a_2 \cdots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \cdots a_1^{-1}.$$

□

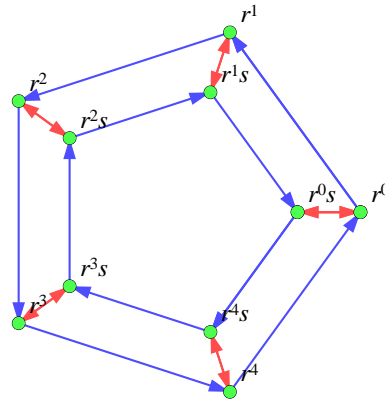
Definition 2.22 (Generators). If S is a subset of a group G such that $G = \langle S \rangle$, we say that S is a set of *generators* of G .

Definition 2.23 (Cayley digraph). For a group G with a generator set S , the *Cayley digraph* is a directed graph which has G as the set of vertices for each pair $(g, s) \in G \times S$ there is an arc labelled s from g to gs .

Remark 2.24. We can easily see that the Cayley digraph is connected, since S is a set of generators. In fact, we can use this in order to verify that S generates G .

Furthermore, from each vertex, there are exactly $|S|$ arcs going out and between any two vertices, there is at most one arc in each direction.

Example 2.25. The dihedral group D_{2n} is generated by one reflection s and one basic rotation r by an angle $2\pi/n$. Thus we can use the generating set $S = \{s, r\}$ and draw the corresponding Cayley digraph. There will be two-way arcs between r^i and $r^i s$ and there will be arcs labelled by r from r^i to r^{i+1} and from $r^i s$ to $r^{i-1} s$. We draw this for $n = 5$ below.



RECOMMENDED EXERCISES

I-5 Subgroups. 8-13, 14-19, 39, 46, 47, 51, 53, 55

I-6 Cyclic groups. 32, 33-37, 45, 46, 48

I-7 Cayley digraphs. 7-11

REFERENCES

- [1] J. B. Fraleigh. *A First Course In Abstract Algebra*. Addison Wesley, seventh edition, 2003.