ALEGBRA I - SUMMARY

YANNIS BÄHNI

Contents

1. Groups

1.1. Subgroups.

Definition 1.1. *A* subgroup *of a group G is a subset $H \subseteq G$ such that*

(1) $1 \in H$

(2) $x \in H$ *implies* $x^{-1} \in H$

(3) $x, y \in H$ *implies* $xy \in H$

Proposition 1.1. *$H \leq G$ if and only if $H \neq \varnothing$ and $x, y \in H$ implies $xy^{-1} \in H$.*

Proposition 1.2. *For $H \neq \varnothing$ the following conditions are equivalent:*

(1) $H \leq G$

(2) $HH \subseteq H$ *and* $H^{-1} \subseteq H$

(3) $HH^{-1} \subseteq H$

(Yannis Bähni) University of Zurich, Rämistrasse 71, 8006 Zurich
E-mail address: yannis.baehni@uzh.ch.

Yannis Bähni
yannis.baehni@uzh.ch

Definition 1.2. *Let G be a group and $X \subseteq G$. Define*

$$\langle X \rangle := \bigcap_{X \subseteq H \leq G} H \tag{1}$$

Proposition 1.3. *Let X be a subset of a group G. Then*

$$\langle X \rangle = \{x_1 \cdots x_n : \forall i \in I \; x_i \in X \cup X^{-1}, n \in \mathbb{N}\} \tag{2}$$

1.1.1. Normal Subgroups.

1.2. Homomorphisms.

Proposition 1.4. *If $\varphi : A \to B$ is a group homomorphism, then $\varphi(1) = 1$, $\varphi(x^{-1}) = \varphi(x)^{-1}$ and $\varphi(x^n) = \varphi(x)^n$ for all $x \in A$ and $n \in \mathbb{Z}$.*

Proposition 1.5. *A group homomorphism $\varphi : A \to B$ is injective if and only if $\ker(\varphi) = \{1\}$.*

Lemma 1.1. *Let $\varphi : G \to H$ be an injective group homomorphism and let $a \in G$ be of finite order. Then $|\langle \varphi(a) \rangle| = |\langle a \rangle|$.*

Proposition 1.6. *If $G = \langle X \rangle$ and $\varphi, \psi : G \to G'$ are group homomorphisms with $\varphi(x) = \psi(x)$ for every $x \in X$ then $\varphi = \psi$.*

1.3. Cyclic Groups.

Definition 1.3. *A group or subgroup is* cyclic *when it is generated by a single element.*

Lemma 1.2. *Every group of prime order is cyclic.*

Proposition 1.7. *Every subgroup of $(\mathbb{Z}, +)$ is cyclic, generated by a unique nonnegative integer.*

Proof. Let $H \leq \mathbb{Z}$. If $H = \{0\}$, then $H = \langle 0 \rangle$. So assume $H \neq \{0\}$. Thus H contains a nonzero integer. Since $H \leq \mathbb{Z}$ we have that H contains a positive integer. Let us denote the smallest positive integer in H by n. Every integer multiple of n belongs to H. Conversely, if $m \in H$ we have by integer division $m = nq + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < n$. So $m - nq = r \in H$ contradicting the minimality of n being the smallest positive integer. Hence $m = nq$ and so $m \in \langle n \rangle$. $\square$

Proposition 1.8. *Let G be a group and let $a \in G$. If $a^m \neq 1$ for all $m \neq 0$, then $\langle a \rangle \cong \mathbb{Z}$; in particular $\langle a \rangle$ is infinite. Otherwise, there is a smallest positive integer n such that $a^n = 1$, and then $a^m = 1$ if and only if n divides m, and $\langle a \rangle \cong \mathbb{Z}/n\mathbb{Z}$; in particular, $\langle a \rangle$ is finite of order n.*

Yannis Bähni
yannis.baehni@uzh.ch

Corollary 1.1. *Any two cyclic groups of order n are isomorphic.*

Corollary 1.2. *Every subgroup of a cyclic group is cyclic. Furthermore, either $H = \{1\}$ or $H = \langle x^n \rangle$, where n is the least positive integer with $x^n \in H$.*

Proof. Let $H \leq G := \langle x \rangle$, $H \neq \{1\}$. Then $H' := \{k \in \mathbb{Z} : x^k \in H\} \leq (\mathbb{Z}, +)$ since

- $0 \in H'$ by $1 = x^0 \in H \leq G$;
- If $k, k' \in H'$ then $k + k' \in H'$ by $x^{k+k'} = x^k x^{k'} \in H$;
- If $k \in H'$ then also $-k \in H'$ by $x^{-k} = (x^k)^{-1} \in H$.

Therefore $H' = \langle n \rangle$ for the least positive integer in H'. Now consider $\langle x^n \rangle$. We have that $\langle x^n \rangle \subseteq H$ by the previous observation and if $x^k \in H$ for some $k \in \mathbb{Z}$ we have $k \in H' = \langle n \rangle$ and so $k = mn$ for some $m \in \mathbb{Z}$ which yields $x^k = x^{mn} = (x^n)^m \in \langle x^n \rangle$. □

Proposition 1.9. *A cyclic group $G := \langle x \rangle$ of finite order n has a unique subgroup of order d, namely $\langle x^{n/d} \rangle = \{g \in G : g^d = 1\}$, for every divisor d of n.*

Proof. We prove the equality $\langle x^{n/d} \rangle = \{g \in G : g^d = 1\}$ only. An element of $\langle x^{n/d} \rangle$ has the form $x^{kn/d}$ for some integer k. Therefore

$$(x^{kn/d})^d = (x^n)^k = 1^k = 1$$

Conversly if $g \in G$ with $g^d = 1$ we have that $g = x^k$ for some integer k since G is cyclic. Hence $1 = g^d = x^{kd}$ and so $n \mid kd$. So

$$g = x^k = (x^{kd/n})^{n/d} = (x^{n/d})^{kd/n} \in \langle x^{n/d} \rangle$$

□

Lemma 1.3. *For all $n \in \mathbb{N}$*

$$\mathbb{Z}_n^\times = \{\overline{k} : \gcd(n, k) = 1\} \qquad \textit{and} \qquad |\mathbb{Z}_n^\times| = \varphi(n)$$

1.4. Symmetric Groups.

1.4.1. Cycles.

Lemma 1.4. *Let*

1.5. Automorphisms.

Definition 1.4. *Let G be a group. For $a \in G$ define*

$$\iota_a : \begin{cases} G \to G \\ x \mapsto axa^{-1} \end{cases} \tag{3}$$

Further

Yannis Bähni
yannis.baehni@uzh.ch

$$\mathrm{Inn}(G) := \{\iota_a : a \in G\} \tag{4}$$

Lemma 1.5. *We have $\iota_a \in \mathrm{Aut}(G)$ for any $a \in G$. Furthermore $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$.*

Proof. $\iota_a \in \mathrm{Aut}(G)$ and $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$ is obvious. Let $\iota_a \in \mathrm{Inn}(G)$ and $\varphi \in \mathrm{Aut}(G)$. Then for $x \in G$

$$\varphi\iota_a\varphi^{-1}(x) = \varphi(a\varphi^{-1}(x)a^{-1}) = \varphi(a)x\varphi(a)^{-1}$$

so $\varphi\iota_a\varphi^{-1} = \iota_{\varphi(a)} \in \mathrm{Inn}(G)$. □

Lemma 1.6. *The mapping*

$$\iota : \begin{cases} G \to \mathrm{Aut}(G) \\ a \mapsto \iota_a \end{cases} \tag{5}$$

is a homomorphisms. Furthermore $\ker(\iota) = Z(G)$.

Proof. That $\iota \in \mathrm{Hom}(G, \mathrm{Aut}(G))$ is obvious. For $a \in \ker(\iota)$ we must have that $\iota_a = \mathrm{id}$, so $axa^{-1} = x$ for any $x \in G$. Hence $a \in Z(G)$. The converse is trivial. □

Thus by the first isomorphism theorem we have

$$G/Z(G) \cong \mathrm{Inn}(G)$$

Proposition 1.10. *Let G be a group and assume $G/Z(G)$ is cyclic. Then G is abelian.*

Proof. Since $G/Z(G)$ is cyclic we have $G/Z(G) = \langle gZ(G)\rangle$ for some $g \in G$. Furthermore, each element of $G/Z(G)$ has the form $(gZ(G))^k = g^kZ(G)$ since $Z(G) \trianglelefteq G$ and $k \in \mathbb{Z}$. Let $x, y \in G$. Since $G/Z(G)$ provides a partition of G we have $x = g^m z$ and $y = g^n z'$ for some $m, n \in \mathbb{Z}$, $z, z' \in Z(G)$. Therefore

$$xy = g^m z g^n z' = g^m g^n zz' = g^{m+n}zz' = g^n g^m zz' = g^n g^m z'z = g^n z' g^m z = yx$$

since center elements commute with every group element. □

1.6. Direct Products.

Proposition 1.11. *A group G is isomorphic to the direct product $G_1 \times G_2$ of two groups G_1, G_2 if and only if it contains normal subgroups $A \cong G_1$ and $B \cong G_2$ such that $A \cap B = \{1\}$ and $AB = G$.*

Lemma 1.7. *Let G be a group. For every $a \in G$ the mappings*

$$\vartheta_a : \begin{cases} G \to G \\ x \mapsto ax \end{cases} \qquad \vartheta'_a : \begin{cases} G \to G \\ x \mapsto xa \end{cases} \tag{6}$$

are bijections.

Yannis Bähni
yannis.baehni@uzh.ch

Theorem 1.1.

Lemma 1.8. *Let G be a group. If $x^2 = 1$ for every $x \in G$ then G is abelian.*

Proposition 1.12. *In a finite group, the inverse of an element is a positive power of that element.*

Proposition 1.13. *If $G = \langle X \rangle$ and the elements of X are pairwise interchangeable then G is abelian. Hence every cyclic group is abelian.*

Definition 1.5. *Let G be a group. The* order of an element *$x \in G$ is defined by $|\langle x \rangle|$.*

Definition 1.6. *Relative to $H \leq G$ the* left coset *of an element $x \in G$ is the subset xH of G; the* right coset *of an element $x \in G$ is the subset Hx of G.*

Proposition 1.14. *The left cosets of $H \leq G$ constitute a partition of G and so do the right cosets.*

Proposition 1.15. *The number of left cosets of a subgroup is equal to the number of right cosets.*

Definition 1.7. *The* index *$[G : H]$ of $H \leq G$ is the cardinal number of its left or right cosets.*

Proposition 1.16. (Lagrange's Theorem) *If $H \leq G$, then $|G| = [G : H]|H|$. Hence if $|G| < \infty$, the order and the index of a subgroup divide the order of G.*

Theorem 1.2. *In a finite group G we have $g^{|G|} = 1$ for any $g \in G$.*

Definition 1.8. *Let $N \trianglelefteq G$. The group of all cosets of N is the* quotient group *G/N of G by N. The homomorphism $x \mapsto xN = Nx$ is the* canonical projection *of G onto G/N.*

Proposition 1.17. *Let $N \trianglelefteq G$. Every subgroup of G/N is the quotient H/N of a unique subgroup H of G that contains N.*

Yannis Bähni
yannis.baehni@uzh.ch

2. Rings

Definition 2.1. *An algebraic structure $(R, +, \cdot)$ with binary operations $+, \cdot : R \times R \to R$ is called a **ring** if $(R, +)$ is an ableian group, $(R, \cdot)$ is a semigroup and for all $x, y, z \in R$ it holds that*

$$x(y+z) = xy + xz \qquad \text{and} \qquad (x+y)z = xz + yz.$$

Definition 2.2. *Let R be a ring. A subset $S \subseteq R$ is called **subring** if $(S, +) \leq (R, +)$ and $xy \in S$ for every $x, y \in S$. If R is a ring with unity, then also $1 \in S$.*

Definition 2.3. *A commutative ring R with unity is called an **integral domain** if it has one of the following equivalent properties:*

(i) (Cancellation) *$zx = zy$ implies $x = y$ for any $x, y, z \in R$ with $z \neq 0$.*
(ii) (No divisors of zero) *$xy = 0$ implies either $x = 0$ or $y = 0$ for any $x, y \in R$.*

Definition 2.4. *A ring R with unity is called a **skew field** if $R^\times = R \setminus \{0\}$.*

Definition 2.5. *A commutative skew field is called a **field**.*

Definition 2.6. *A ring $R \neq \{0\}$ is called **simple** if (0) and R are the only ideals.*

Definition 2.7. *Let R be a commutative ring. An ideal $P \neq R$ is called a **prime ideal** if $ab \in P$ implies either $a \in P$ or $b \in P$ for $a, b \in R$.*

Lemma 2.1. *An ideal $P \neq R$ of a commutative ring R with unity is a prime ideal if and only if R/P is an integral domain.*

Definition 2.8. *An ideal $M \neq R$ is called **maximal** if there exists no ideal I such that $M \subsetneq I \subsetneq R$.*

Lemma 2.2. *Let R be a commutative ring with unity. An ideal $M \neq R$ is maximal if and only if R/M is a field.*

Definition 2.9. *An integral domain R is called a **factorial domain** or **unique factorisation domain** when the following properties hold:*

(i) Every element $x \notin R^\times \cup \{0\}$ can be written as product of irreducible factors.
(ii) If $p_1 \cdots p_n = q_1 \cdots q_m$ for irreducible $p_1, \ldots, p_n, q_1, \ldots, q_m \in R$, then $n = m$ and there exists $\sigma \in S_n$ such that $p_i \sim q_{\sigma(i)}$ for $i = 1, \ldots, n$.

Definition 2.10. *An integral domain is called a **principal ideal domain** if every ideal of R is principal.*

Yannis Bähni
yannis.baehni@uzh.ch

Theorem 2.1. *Every principal ideal domain is a factorial domain.*

Definition 2.11. *An integral domain R is called an* ***euclidean domain*** *if there is a mapping $\varphi : R \setminus \{0\} \to \mathbb{N}_0$ with the following property: To any $a, b \in R$ with $b \neq 0$ there exist $q, r \in R$ such that $a = qb + r$ and either $r = 0$ or $\varphi(r) < \varphi(b)$.*

Theorem 2.2. *Every euclidean domain is a principal ideal domain.*

Definition 2.12. *A ring R is called* ***noetherian*** *if it has one of the following equivalent properties:*

- (i) *Every ascending chain $A_1 \subseteq A_2 \subseteq \dots$ of ideals A_i of R is stationary, i.e. there exists some $k \in \mathbb{N}$ such that $A_i = A_k$ for every $i \geq k$.*
- (ii) *Every nonempty collection of ideals of R contains a maximal element.*
- (iii) *Every ideal of R is finitely generated.*

Theorem 2.3. (Hilbert) *If R is a commutative noetherian ring with unity then $R[X]$ is noetherian.*

Yannis Bähni
yannis.baehni@uzh.ch

3. Usefull Stuff

- Let G be a group and $H, K \leq G$. Then
$$[G : (H \cap K)] \leq [G : H] [G : K] . \tag{7}$$
- Consider the system of congruence equations
$$X \equiv a_1 \bmod r_1, \ldots, X \equiv a_n \bmod r_n \tag{8}$$
where $r_1, \ldots, r_n \in \mathbb{Z}$ are pairwise coprime and $a_1, \ldots, a_n \in \mathbb{Z}$. Now set
$$r := r_1 \cdots r_n \qquad \text{and} \qquad s_i := \frac{r}{r_i} \tag{9}$$
for each $i = 1, \ldots, n$ and determine $k_i \in \mathbb{Z}$ such that
$$k_i s_i \equiv 1 \bmod r_i \tag{10}$$
for each $i = 1, \ldots, n$. This can be done using the extended euclidean algorithm, i.e. since s_i and r_i are coprime, we find $t_i \in \mathbb{Z}$ such that
$$k_i s_i + t_i r_i = 1. \tag{11}$$
Then
$$k := k_1 s_1 a_1 + \cdots + k_n s_n a_n \tag{12}$$
is a solution of (8) and the set of solutions of (8) is $k + r\mathbb{Z}$.