Vorlesung aus dem WS21/22

Algebra

Prof. Dr. N. S.

geTEXt von Ningh

Contents

1 Gruppentheorie

1.1 Grundbegriffe der Gruppentheorie

Definition 1.1 (Gruppe). A group is a set G together with a binary operation on G, here denoted "$\cdot$", that combines any two element a and b to from an element of G, denoted by $a \cdot b$, such that following three requirements, known as group axiom, are statisfied:

- Associativity: $\forall a, b \in G : (a \cdot b) \cdot c = a \cdot (b \cdot c)$
- Identity element: $\exists e \in G \forall a \in G : a \cdot e = e \cdot a = a$
- Inverse element: $\forall a \in G \exists b \in G : a \cdot b = e$

Remark 1.2. The definition of a group don't require that $\forall a, b \in G : a \cdot b = b \cdot a$. If this additional condition holds, then the operation is said to be commutative, and the group is called an abelian group.

Following are some basic properties of group. Proof would not be repeated here.

Proposition 1.3.

- *The neutral element is unique.*
- *Inverse in group is unique.*

Example 1.4. The direct product: Let G_1, G_2 be groups. Let $G_1 \times G_2$ be the direct product as sets. We can define the product componentwise by $(x_1, x_2)(y_1, y_2) = (x_1 y_1, x_2 y_2)$. Then $G_1 \times G_2$ is a group, whose unit element is (e_1, e_2).

Definition 1.5 (Subgroup). Let G be a group. A subgroup H of G is a subset of G containing the unit element, and such that H is closed under the law of composition and inverse.

Remark 1.6. A subgroup is called trivial if it consists of the unit element alone.

Definition 1.7 (Generator). Let G be a group and S be a subset of G. We shall say that S generates G, or that S is a set of generators for G, if every element G can be expressed as a product of elements of S or inverses of elements of S, i.e. as a product $x_1 \cdots x_n$ where each x_i or x_i^{-1} is in S.

Remark 1.8.

- It is clear that the set of all such products is subgroup of G, and is the smallest subgroup of G containing S.
- S generates G iff the smallest subgroup of G containing S is G itself. If G is generated by S, then we write $G = \langle S \rangle$
- By definition, a cyclic group is a group which has one generator.
- Given elements $x_1, \cdots, x_n \in G$, these elements generate a subgroup $\langle x_1, \cdots, x_n \rangle$, namely the set of all element of G of the form

$$x_{i_1}^{k_1} \cdots x_{i_r}^{k_r} \text{ with } k_1, \cdots, k_r \in \mathbb{Z}$$

- A single element $x \in G$ generates a cyclic subgroup.

Lemma 1.9. *Let H a nonempty subset of G. If $a^{-1}b \in H$ for all $a, b \in H$, H is a subgroup of G.*

Definition 1.10 (Grouphomomorphism). Let G, G' be groups. A grouphomomorphism of G into G' is a mapping $f : G \longrightarrow G'$ such that $f(xy) = f(x)f(y)$ for all $x, y \in G$.

Remark 1.11.

- Let $f : G \longrightarrow G'$ be a grouphomomorphism. Then $f(x^{-1}) = f(x)^{-1}$ and $f(e) = e'$.
- Composition of homomorphism is homomorphism.
- A homomorphism $f : G \longrightarrow G'$ is called an isomorphism if there exists a homomorphism $g : G' \longrightarrow G$ such that $f \circ g,\ g \circ f$ are the identity mapping. Obviously f is isomorphism iff f is bijective. The existence of an isomorphism between two group G and G' is sometimes denoted $G \sim G'$. If $G = G'$,we say that isomorphism is an automorphism. A Homomorphism of G into itself is also called an endomorphism.

Definition 1.12 (Kernel and image). Let $f : G \longrightarrow G'$ be a grouphomomorphism. Let e, e' be the respective unit element of G, G'. We define the kernel of f be the subset of G consisting of all x such that $f(x) = e'$. Let H' be the image of f.

Remark 1.13.

- From the definition, it follows at once that the kernel H of f is a subgroup G. H' is a normal subgroup of G'.
- The kernel and image of f are sometimes denoted by $\ker f$ and $\operatorname{im} f$.
- A homomorphism whose kernel is trivial is injective.

Definition 1.14 (Centralizer). Define $C_G(A) = \{g \in G \mid gag^{-1} = a \text{ for all } a \in A\}$. This subset of G is called the centralizer of A in G. Since $gag^{-1} = a$ if and only if $ga = ag$, $C_G(A)$ is the set of elements of G which commute with every element of A.

Remark 1.15. Centralizer is subgroup.

Definition 1.16 (Center). Define $Z(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}$, the set of elements commuting with all the elements of G. This subset of G is called the center of G.

Remark 1.17. Note that $Z(G) = C_G(G)$, so the argument above proves $Z(G) \leqslant G$ as a special case.

Definition 1.18 (Normalizer). Definition. Define $gAg^{-1} = \{gag^{-1} \mid a \in A\}$. Define the normalizer of A in G to be the set $N_G(A) = \{g \in G \mid gAg^{-1} = A\}$.

Remark 1.19. Notice that if $g \in C_G(A)$, then $gag^{-1} = a \in A$ for all $a \in A$ so $C_G(A) \leqslant N_G(A)$.

Definition 1.20 (Coset). Let G be a group and H a subgroup. A left coset of H is G is a subset of G og type aH for some element a of G.

$$aH := \{ab : b \in H\}$$

Any element of a coset is called a representative for the coset.

Lemma 1.21. *Let N be any subgroup of the group G. The set of left cosets of N in G form a parition of G. Furthermore, for all $u, v \in G$. Furthermore, for all $u, v \in G, uN = vN$ iff $v^{-1}u \in N$, and in particular, $uN = vN$ iff u and v are representatives of the same coset.*

Proposition 1.22. *Let G be a group and let N be a subgroup of G.*

- *The operation on the set of left cosets of* N *in* G *described by*

$$uN \cdot vN = (uv)N$$

is well defined if and only if $gng^{-1} \in N$ *for all* $g \in G$ *and all* $n \in N$.

- *If the above operation is well defined, then it makes the set of left cosets of* N *in* G *into a group. In particular the identity of this group is the coset* $1N$ *and the inverse of* gN *is the coset* $g^{-1}N$ *i.e.,* $(gN)^{-1} = g^{-1}N$.

Definition 1.23 (normal). The element gng^{-1} is called the conjugate of $n \in N$ by g. The set $gNg^{-1} = \{gng^{-1} \mid n \in N\}$ is called the conjugate of N by g. The element g is said to normalize N if $gNg^{-1} = N$. A subgroup N of a group G is called normal if every element of G normalizes N, i.e., if $gNg^{-1} = N$ for all $g \in G$. If N is a normal subgroup of G we shall write $N \trianglelefteq G$.

Remark 1.24.

- $N \trianglelefteq G \Leftrightarrow \forall a \in G : aNa^{-1} = N \Leftrightarrow \forall a \in G : aNa^{-1} \subset N$ $(\forall g : H = g(g^{-1}Hg)g^{-1} \subset gHg^{-1} \subset H)$
- Aber es gilt $gHg^{-1} \subset H \not\Rightarrow gHg^{-1} = H$

Theorem 1.25. *Let* N *be a subgroup of the group* G. *The following are equivalent:*

(i) $N \trianglelefteq G$
(ii) $N_G(N) = G$
(iii) $gN = Ng$ *for all* $g \in G$
(iv) gNg^{-1} *for all* $g \in G$.

FIXME:zhe TM sha,shuizhidaotacongnalikaishidingyia TODO: QUOTIENT GROUP.
Hier sollten die Definition von Faktorgruppen sein. Aber ich weisse nicht wie ich das machen kann.

Definition 1.26 (Faktorgruppe).

Theorem 1.27 (Fundamental theorem on homomorphisms). *Let* $\phi : G \longrightarrow G'$ *be a grouphomomorphism and* $N \trianglelefteq G$ *with* $N \subset \ker \varphi$. *There is a unique grouphomomorphism*

$$\bar{\varphi} : G/N \longrightarrow G'$$

, such that

$$\begin{tikzcd} G \arrow[rr, "\varphi"] \arrow[dr, "\pi"] & & G' \\ & G/N \arrow[ur, "\bar{\varphi}"] & \end{tikzcd}$$

commute.

In particular

$$G/\ker f \simeq \operatorname{im} f \leqslant G'$$

.

Proof is egal.
TODO: Also you should know what is order of a element in a group. But I just don't know where should i write that.

THEOREM 1.28 (Universelle Eigenschaft der Faktorgruppe). *Let* G *be a group,* N *a normal subgroup* $N \trianglelefteq G$, π *canonical projection* $\pi : G \longrightarrow G/N, g \longmapsto gN$. *Then*

$$\varphi \textit{ factorize the quotient group } G/N(\textit{i.e. } \exists\bar{\varphi} : G/N \longrightarrow G' \textit{ Homo.}) \Leftrightarrow N \subset \ker\varphi$$

.

Notice:

$$\begin{tikzcd} G \arrow[rr, "\pi"] \arrow[dr, "\varphi"'] & & G/N \arrow[dl, "\exists\bar{\varphi}"] \\ & G' & \end{tikzcd}$$

TODO: I think I still need proof of lagrange theorem here. Maybe I do it later.

1.2 Konjugationsklasse, Automorphism, semidirekt Produkt

TODO:zhi hou zai xie ba .

1.3 Kommutatoruntergruppe

Definition 1.29. Let G be a group, let $x, y \in G$ and let A, B be nonempty subsets of G.

- Define $[x, y] = x^{-1}y^{-1}xy$, called the commutator of x and y.
- Define $[A, B] = \langle [a, b] \mid a \in A, b \in B\rangle$, the group generated by commutators of elements from A and from B.
- Define $G' = \langle [x, y] \mid x, y \in G\rangle$, the subgroup of G generated by commutators of elements from G, called the commutator subgroup of G.

Remark 1.30. We don't have $\langle [x, y] \mid x, y \in G\rangle = [[x, y] \mid x, y \in G]$ in general. You can find a counterexample in Uebungsblatt.

Theorem 1.31. *Let G be a group.* $[G, G] \trianglelefteq G$, *and* $G^{ab} := G/[G, G]$ *is abelian.*

The proof is straightforward. And I think we don't need to know many detail of commutator in this lecture.

Theorem 1.32. *Let G be a group, $\pi : G \longrightarrow G^{ab}$ canonical projection. $\varphi : G \longrightarrow A$ a grouphomomorphism with a abelian group A. There is a unique homomorphism $\bar{\varphi} : G^{a}b \longrightarrow A$ with $\varphi = \bar{\varphi} \circ \pi$.*

I am not interested in this. Is comes directly from Universelle Eig. der Faktorgruppen. Normal subgroup is subset of kernel is statisfied, because A is abelian. Proof is egal.

$$\begin{tikzcd}
G \arrow[rr, "\pi"] \arrow[dr, "\varphi"'] & & G^{ab} = G/[G, G] \arrow[dl, "\exists\varphi"] \\
& A &
\end{tikzcd}$$

Definition 1.33. G is perfect, if $G = [G, G]$.

Example 1.34. $\mathrm{sgn} : S_n \longrightarrow \pm 1$. Clearly ± 1 is abelian. Then it holds $[S_n, S_n] \subset \mathrm{sgn} = A_n$. And A_n is generated by 3-cycle, so $A_n \subset [S_n, S_n]$.

FIXME: I am not pretty sure what this example talks about.

1.4 Endliche ableische Gruppe

Herr S. just give 2 theorem here. No motivation and no explanation. Nothing is more confusing than this. I have totally no idea what is going on. And I dont know what should i write down.

1.5 Gruppenwirkung

We just define left group action here. Right group action is quite similar.(Actually we don't use it at all)

DEFINITION 1.35 (Left group action). Let G be a group with neutral element e, and X is a set. Then (left) group action s of G on X is a function $s : G \times X \longrightarrow X$, that satisfied the following two axiom:

- $s(e, x) = x$
- $s(g, s(h, x)) = s(gh, x)$

(with $s(g, x)$ often shortened to gx or $g \cdot x$ when the action being considered is clear from context.)

- $ex = x$
- $g(hx) = (gh)x$

for all g and h in G and all x in X.

REMARK 1.36.

- The group G is said to act on X (from the left). A set X together with an action of G is called a (left) G-set.
- You must know the operation in gh and hx is different.

DEFINITION 1.37 (Bahn or orbit). Consider a group G acting on a set X. The orbit of an element x in X is the set of elements in X to which x can be moved by the elements of G. The orbit of x is denoted by Gx.

$$G \cdot x = \{g \cdot x : g \in G\}$$

REMARK 1.38.

The action is transitive iff it has exactly only one orbit, that is, if there exists x in X with $Gx = X$. This is the case iff $Gx = X$ for all x in X.

Two orbit is same or disjoint, because $gx = hy \in Gx \cap Gy \Rightarrow x = g^{-1}hy, alsoGx \subset Gy$ and $y = h^{-1}gx$, also $Gy \subset Gx$. So X is disjoint union of every orbit. (i.e. orbits is a parition.)

Given g in G and x in X with $g \cdot x = x$, $g \cdot x = x$, it is said that "x is a fixed point of g" or that "g fixes x". Then we can defien stabilizer and fixed points.

DEFINITION 1.39 (Stabilizer and fixed points).

- For every x in X, the stabilizer subgroup of G with respect to x is the set of all element in G that fix x. $G_x := \{g \in G \mid gx = x\}$.
- x ist fixed point if $Gx = \{x\}$. X^G is set of all fixed(invariant) point.

REMARK 1.40. The action of G on X is free iff all stabilizer are trivial.

LEMMA 1.41. *Let* $G \times X \longrightarrow X$ *a action of* G *on* X. *Then*

$$|X| = \sum_{B \backslash X} |B|$$

LEMMA 1.42. *Let* $G \times X \longrightarrow X$ *a action of* G *on* X. *For every* $x \in X$ *the function* $\varphi : G \longrightarrow X, g \longmapsto gx$ *can be reduced to a isomorphism* $G/G_x \simeq Gx$, *where* G/G_X *is set of left cosets. In particular it holds* $\mathrm{ord}(Gx) = G : Gx$

Proof. It holds $\varphi(g) = \varphi(h) \Leftrightarrow gx = hx \Leftrightarrow h^{-1}gx = x \Leftrightarrow h^{-1}g \in G_x \Leftrightarrow gG_x = hG_x$
Also φ is a injective function $G \longrightarrow X, g \longmapsto$. Obvioulsy is φ surjective.
Following is something more deteailed.[Fraleigh 16.16 Theorem]

- We define a one-to-one map ϕ from Gx onto the collection of left costes of G_x in G. i.e. $\phi(x_1) = g_1 G_x$
- We need to show that the function ist well defined, injective and surjective.(See the book for detail, it is just calculation).
- If $|G|$ is finite, then the equation $|G| = |G_x|(G : G_x)$ shows that $|Gx| = (G : G_x)$ is a divisor of $|G|$.

□

Theorem 1.43 (Bahnengleicung).

$$|X| = \sum_{i=1}^{r} |Gx_i| = \sum_{i=1}^{r} |G : G_{x_i} of solvable groups are solv|$$

Proof. X is disjoint union of all orbit B_i with $B_i = Gx_i$. Then holds $|X| = \sum_{i=1}^{r} |Gx_i| = \sum_{i=1}^{r} |G : G_{x_i}|$ directly by lemma. □

Lemma 1.44. *Let* $G \times X \longrightarrow X$ *a action of* G *on* X. *If* $x \in X, g \in G$, *then* $G_{gx} = gG_x g^{-1}$

Proof. $h \in G_{gx} \Leftrightarrow hgx = gx \Leftrightarrow g^{-1}hgx = x \Leftrightarrow g^{-1}hg \in G_x \Leftrightarrow h \in gG_x g^{-1}$ □

Remark 1.45. In some skript man can find auch Klassengleichung. It is a special case of Bahnengleichung with respect conjugationfunction and center.

1.6 p-Gruppe

Definition 1.46 (p-group). Let G be a group and let p be a prime.

(i) A group of order p^α for some $\alpha \geqslant 1$ is called a p-group. Subgroup of G which are p-groups are called p-subgroup.

(ii) If G is a group of order $p^\alpha m$, where$|\!\!/m$, then a subgroup of order p^α is called a Sylow p-subgroup og G.

(iii) The set of Sylow p-subgroup of G will be denoted by $\mathrm{Syl}_p(G)$ and the number of Sylow p-subgroup will be denoted by $n_p(G)$.

Lemma 1.47. *Let G be a group of order p^n and let X be a finite G-set. Then $|X| = |X_G| \mod p$.*

Proof. There may be one-element orbit in X. Let $X^G = \{x \in X \mid gx = x \ \ \forall a \in G\}$. Thus X^G is precisely the union of the one-element orbits in X. Let us suppose there are s one-element orbits, where $0 \leqslant s \leqslant r$. Then $|X^G| = s$(reordering the x_i if necessary), then we may rewrite Eq. in 1.43

$$|X| = |X^G| + \sum_{i=s+1}^{r} |Gx_i|$$

Also we know $|Gx_i|$ divides $|G|$ by Lemma 1.42. Consequently p divides $|Gx_i$ for $s+1 \leqslant i \leqslant r$. So $|X| - |X^G|$ is divisible by p, so $|X| = |X^G| \mod p$ □

Theorem 1.48. *Let G be a group of order p^n. Then $Z(G) \neq 1$ and there is a central element of order p (x is of order p^l, then $x^{p^{l-1}}$ has order p).*

Proof. Consider conjugation an action of G on G. Then G is fixed point iff g commutes with all element in G (i.e. $g \in Z(G)$. Also $e \in |Z(G)| = |G| = 0 \mod p$, so $|Z(G)| \geqslant p$. □

Theorem 1.49 (Cauchy's Theorem). *Let p be a prime. Let G be a finite group and let p divide $|G|$. Then G has an element of order p and, Consequently, a subgroup of order p*

Remark 1.50. Herr S. didn't mention this in lecture. But I think it would be better if we know it.

Theorem 1.51. *Let p Be a prime, and G a p-group of order p^k. There is a sequence of subgroup*

$$\{e\} = G_0 < G_1 \cdots < G_n = G \ \ \textit{with} \ \ |G_i| = p^i \wedge \forall i: \ G_i \trianglelefteq G$$

Proof. We can use the induction on natural number here. For $k = 1$ it is trivial. Let $k > 1$. By Theorem 1.48 we can find a central element a of order p. The quotient group $\bar{G} = G/(a)$ is of order p^{k-1}. □

Theorem 1.52 (Sylow). *Let G be a finite group of order $p^\alpha m$, where p is a prime, $m \geqslant 1$, and p does not divide m. Then:*

(i) $\mathrm{Syl}_p(G) \neq \emptyset$, *i.e. Sylow p-subgroups exist!*

(ii) $n_p(G) = 1 \mod p \wedge n_p(G) \mid m$

(iii) *Any p-subgroup of G is contained in a Sylow p-subgroup.*

(iv) *Any Sylow p-subgroups are conjugate in G, i.e. P_1 and P_2 are both Sylow p-subgroups, then there is some $g \in G$ such that $P_1 = gP_1g^{-1]}$. In particular $n_p(G) = (G : N_G(P))$.*

Remark 1.53. Attention: Herr S. use symbol s_p for the number of Sylow p-subgroup. (Just notation.)

Proof. Whatever.FIXME: □

1.7 Auflösbare Gruppe

Definition 1.54 (Derived series). This construction can be iterated:

$$G^{(0)} := G$$

$$G^{(n)} := [G^{(n-1)}, G^{(n-1)}]$$

The groups

$$G^{(2)}, G^{(3)}, \dots$$

are called the second derived subgroup, third derived subgroup, and so forth the descending normal series $\cdots \trianglelefteq G^{(2)} \trianglelefteq G^{(1)} \trianglelefteq G^{(0)} = G$ is called derived series.

Definition 1.55. A group is called solvable, if its derived series, the descending normal series, where every subgroup is the commutator subgroup of the previous one, eventually reaches the trivial subgroup of G.

Remark 1.56. In many book there is equivalent definition: A group G solvable if it has a subnormal series whose factor groups (quotient groups) are all abelian, that is, if there are subgroups $1 = G_0 < G_1 < \cdots < G_k = G$ such that G_{j-1} is normal in G_j, and G_j/G_{j-1} is an abelian group, for $j = 1, 2, \dots, k$. A proof to this could be found in Dummit Sec. 6.1 Theorem 9.

Proposition 1.57. *Let G and K be groups, let H be a subgroup of G and let $\varphi : G \longrightarrow K$ be a surjective homomorphism.*

- $H^{(i)} \leqslant G^{(i)}$ *for all $i \geqslant 0$. In particular, if G is solvable, then so is H, i.e. subgroups of solvable groups are solvable (and the solvable length of H is less than or equal to the solvable length of G). .*
- $\varphi(G^{(i)}) = K^{(i)}$. *In particular, homomorphic images and quotient groups of solvable groups are solvable (of solvable length less than or equal to that of the domain group).*
- *If N is normal in G and both N and G/N are solvable then so is G.*

Theorem 1.58. *All p-Gruppe is solvable.*

Theorem 1.59. *Let p, q be prime with $p < q$. Group of order pq is solvable (for $p = q$ it is even abelian).*

Proof. Let G be a group of order pq, wlog $p < q$, s be the number of q-sylowsubgroup in G. We have $s \mid p \wedge s = 1 \mod q \Rightarrow s = 1$. There is a unique q-sylowsubgroup U and U is normal in G. So U is group of order of q and G/U is group of order of p. By theorem 1.58, they are both solvable, so G is solvable. □

Theorem 1.60. *Let p, q, r be prime with $p < q < r$. Group of order pqr is solvable.*

Proof. If G has only one sylowsubgroup for p, q, r, then is the sylowsubgroup normal and the quotient group is solvable by proposition 1.57. Then is G directly solvable by previous Theorem.
Otherwise, assume there are more than $q + 1$ q-sylowsubgroup and pq r-sylowsubgroup. So G have more than $(q + 1)(q - 1)$ element of order q and $pq(r - 1)$ element of order r. Then G have at least $pq(r - 1) + (q + 1)(q - 1) + 1 = pqr + q(q - p) > pqr = |G|$. This lead to a contradiction. □

1.8 Composition series

Definition 1.61 (Simple group). A simple group is a nontrivial group whose only normal subgroup are the trivial group and the groups itself.

Definition 1.62. A composition series of a group G is a subnormal series of finite length

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = G$$

with strict inclusions, such that each H_i is a maximal proper normal subgroup of H_{i+1}.

Theorem 1.63. (i) *The Schreier refinement theorem of group theory states that any two subnormal series of subgroups of a given group have equivalent refinements, where two series are equivalent if there is a bijection between their factor groups that sends each factor group to an isomorphic one.*

(ii) *The Jordan–Hölder theorem (named after Camille Jordan and Otto Hölder) states that any two composition series of a given group are equivalent.*

Remark 1.64. Noproof, whatever.

1.9 Einfach Gruppen

THEOREM 1.65. *(Galois)* A_n *ist für* $n \geqslant 5$ *einfach.*

Proof. TODO: □

LEMMA 1.66. *Die einzigen Normalteiler von* S_n *sind 1,* A_n *und* S_n.*(*$n \geqslant 5$ *sonst falsch)*

2 Ringe

Definition 2.1 (Ring). (i) A ring R is a set together with two binary operation $+$ and $\times$ (called addition adn multplication) satisfying the following axioms:

- $(R, +)$ is an ableian group.
- $\times$ is associative: $a \times (b \times) = (a \times b) \times c$ for all $a, b, c \in R$
- the distributive laws hold in R: for all $a, b, c \in R$:

$$(a + b) \times c = (a \times c) + b \times c \ \text{ and } \ a \times (b + c) = (a \times b) + (a \times c)$$

(ii) The ring R is commutative if multplication is commutative.

(iii) The ring R is said to have an identity (or contain a 1) if there is an element $1 \in R$ with

$$1 \times a = a \times 1 = a \ \text{ for all } \ a \in R$$

(iv) A subring of the ring R is a subgroup of R that is closed under multplication.

Following are some basic properties of ring. Proof would not be repeated here.

Proposition 2.2. *Let R be a ring. then*

- $0a = a0 = 0$ *for all* $a \in R$.
- $(-a)b = a(-b) = -(ab)$ *for all* $a, b \in R$.
- $(-a)(-b) = ab$ *for all* $a, b \in R$.
- *If R has an identity, then the identity is unique and* $-a = (-1)a$.

Definition 2.3. (i) A nonzero element a of R is called zero divisor if there is a nonzero element b in R such that either $ab = 0$ or $ba = 0$.

(ii) Assume R has an identity $1 \neq 0$. An element u of R is called a unit in R if there is some v in R such that $uv = vu = 1$. The sets of units in R is denoted $R^\times$

Remark 2.4. In this terminology a field is a commutative ring F with identity $1 \neq 0$ in which every nonzero element is a unit, i.e. $F^\times = F - \{0\}$

Definition 2.5 (Integral domain). A commutative ring with identity $1 \neq 0$ is called an integral domain if it has no zero divisors.

Remark 2.6. Assume a, b, b are elements of any ring with a not a zero divisor. If $ab = ac$, then either $a = 0$ or $b = c$.

Remark 2.7. Here should be the definition of ringhomomorphism and some basic properties. It is very similar to group. I am not going to write everything down here. See Dummit if necessary

Definition 2.8 (Ideal). Let R be a ring, let I be a subset of R and let $r \in R$.

(i) $rI = \{ra \mid a \in I\}$ and $Ir = \{ar \mid a \in I\}$

(ii) A subset I of R is a left ideal of R if

  (i) I is a subring of R, and

  (ii) I is cloed under left multplication by elements from R, i.e. $rI \subset I$ for all $r \in R$

Right ideal is similar.

(iii) A subset I that is both a left and a right ideal is called an ideal of R.

Remark 2.9. Let R be a ring and let I be an ideal of R. Then the (additive) quotient group R/I is a ring under the binary operation:

$$(r+I)+(s+I)=(r+s)+I \quad (r+I)\times(s+I)=(rs)+I$$

for all $r, s \in R$. Conversely, if I is any subgroup such that the above operations are well defined, then I is an ideal of R.

TODO:IOS SATZ VON RING.

2.1 Euklidische Ringe

This is followed by lecture notes from Linear Algebra II by Prof. W. B.

2.1.1 Elementare Teilbarkeitslehre

Im weiteren sei R stets ein kommutativer Ring mit 1. Unsere wichtigsten Beispiel sind der Ring der ganzen Zahlen $\mathbb{Z}$ und der Polynomring $\mathbb{K}[x]$ über einem Körper $\mathbb{K}$.

Definition 2.10. Zwei Element $a, b \in R$ heißen zueinander assoziiert, falls $a|b$ und $b|a$. In Zeichen: $a \sim b$

Lemma 2.11. *Falls* R *nullteilerfrei ist, so gilt*

$$a \sim b \Leftrightarrow \exists e \in R^{\times} : b = ea$$

Proof. " $\Leftarrow$ " $(b = \mu a \Rightarrow a|b) \wedge (\mu^{-1}b = a \Rightarrow b|a) \Rightarrow a \sim b$

" $\Rightarrow$ " $(a|b \Rightarrow \exists e \in R : b = ea) \wedge (b|a \Rightarrow \exists f \in R : a = fb) \Rightarrow fbe = b \Rightarrow b(fe - 1) = 0 \Rightarrow fe = 1 \Rightarrow e, f \in R^{\times}$

□

Für $a \in R$ bezeichnen wie nun mit

$$(a) = aR = \{ra|r \in R\}$$

die Menge aller Vielfachen von a. In einem nullteilerfreien Ring gelten folgende Äquivalenzen:

- $a \mid b \Longleftrightarrow (b) \subseteq (a)$
- $a \sim b \Longleftrightarrow (a) = (b)$
- $(a) = R \Longleftrightarrow a \in R^{\times}$

Definition 2.12. Eine Teilmenge $J \subseteq R$. heift Ideal, falls

- $0 \in J$.
- $a, b \in J \Longrightarrow a + b \in J$
- $a \in J, r \in R \Longrightarrow ra \in J$

Ideale der Form (a) heifen Hauptideale.

Example 2.13. In $\mathbb{Z}$ ist jedes Ideal ein Hauptideal.

Proof. Sei α ein Ideal in $\mathbb{R}$, in Zeichen: $\alpha \triangleleft \mathbb{Z}$. oE $\alpha \neq (0) = 0$. Sei $a := \min(\alpha \cap \mathbb{N})$. z.z.:$(a) = \alpha$.

" $\subseteq$ " $a \in \alpha \Rightarrow \mathbb{Z}a \subseteq \alpha$

" $\supseteq$ " Sei $b \in \alpha$. Teil mit Rest: $b = qa + r, \quad 0 \leqslant r < a \Rightarrow r = b - qa \in \alpha \Rightarrow r = 0 \Rightarrow b = qa \in (a)$

□

Analog: Auch in $\mathbb{K}[x]$ ist jedes Ideal ein Hauptideal.

Definition 2.14. Seien I, J zwei Ideale in R. Dann heißt

- $I+J=\{a+b \mid a \in I, b \in J\}$ die Summe
- $I \cap J$ der Durchschnitt und
- $IJ=\{\sum_{i \text{ end!}} a_i b_i \mid a_i \in I, b_i \in J\}$ das Produkt

der Ideale I und J.

Example 2.15. $R=\mathbb{Z}[x]$. Dann ist $(2)+(x)$ ist kein Hauptideal.

Proof. Angenommen $(2)+(x)=(g),\ g \in \mathbb{Z}[x] \Rightarrow (x) \subseteq (g) \Rightarrow g|x \Rightarrow \deg(g) \leqslant 1 \Rightarrow g(x)=x+1, a \in \mathbb{Z}$ oder $g=\pm 1$„ □

Man beachte, daB Summe, Durchschnitt und Produkt wieder Ideale in R sind.

Definition 2.16. Ein nullteilerfreier Ring heift Hauptidealring, falls jedes Ideal ein Hauptideal ist.

Die Ringe $\mathbb{Z}$ und $K[x]$ sind Hauptidealringe. Tatsächlich sind diese Ringe sogar Beispiele für sogenannte Euklidische Ringe.

Definition 2.17. Ein nullteilerfreier Ring R heiBt euklidisch, falls es eine Abbildung $\nu : R \backslash \{0\} \longrightarrow \mathbb{N}_0$ gibt, so daB gilt: zu $a, b \in R, b \neq 0$, gibt es $q, r \in R$ mit

$$a = qb + r, \quad r = 0 \text{ oder } \nu(r) < \nu(b).$$

Die Abbildung ν nennt man euklidische Norm.

Example 2.18. $R=\mathbb{Z}[i]=\mathbb{Z}[\sqrt{-1}]=\{a+bi \mid a, b \in \mathbb{Z}\}$ ist euklidisch bez $\phi(a+bi) := N(a+bi) = a^2+b^2$.

Theorem 2.19. *Jeder euklidische Ring ist ein Hauptidealring. Definition* 5.1.8 *Seien* $a, b \in R$. *Wir nennen* $d \in R$ *einen gröften gemeinsamen Teiler von* a *und* b, *falls die folgenden zwei Eigenschaften erfullt sind:*

- $d \mid a$ *und* $d \mid b$.
- *Falls* $d_1 \mid a$ *und* $d_1 \mid b$ *für* $d_1 \in R$ *gilt, so gilt auch* $d_1 \mid d$.

Remark 2.20. Ein ggT (falls er existiert) ist bis auf Assoziiertheit eindeutig bestimmt. D.h., sind d_1 und d_2 zwei ggT von a und b, so gibt es eine Einheit $u \in R^\times$ mit $d_1 = ud_2$.

In beliebligen kommutativen Ringen existieren ggT im Allgemeinen nicht. Jedoch gilt der folgende Satz.

Theorem 2.21. *Sei* R *ein Hauptidealring und* $a, b \in R$. *Sei* $(a)+(b)=(d)$. *Dann ist* d *ein* ggT *von a und* b

In euklidischen Ringen verfügen wir über einen Algorithmus zur expliziten Berechnung von $\mathrm{ggT}(a,b)$. Der erweiterte euklidische Algorithmus erlaubt sogar die Berechnung einer Darstellung

$$\mathrm{ggT}(a,b) = xa + yb \text{ mit } x, y \in R\ .$$

2.1.2 Der chinesischer Restsatz

THEOREM 2.22 (Chinesischer Restsatz). *Seien* $I_1, \cdots, I_n$ *Ideale in* R *mit* $I_k + I_l = R$*(koprim) für* $k \neq l$. *Seien* $r_1, \cdots, r_n \in R$. *Dann gibt es ein* $x \in R$ *mit* $x \equiv r_k (\operatorname{mod} I_k)$ *für* $k = 1, \cdots, n$. *Falls* $y \in R$ *eine weitere Lösung dieser simultanen Kongruenzen ist, so gilt* $x \equiv x (\operatorname{mod} J)$*, wobei* $J := I_1 \cap \cdots \cap I_n$. *Zwei verschiedene Lösungen sind also modulo* J *eindeutig bestimmt.*

Proof. TODO: MAYBE LATER>. □

In äquivalenter Weise kann man den chinesischen Restsatz wie folgt formulieren.

THEOREM 2.23. *Seien* $I_1, \ldots, I_n$ *Ideale in* R *mit* $I_k + I_l = R$ *für* $k \neq l$. *Dann ist die Abbildung*

$$\begin{aligned} \varphi : R/J &\longrightarrow \quad R/I_1 \times \ldots \times R/I_n \\ x + J &\longmapsto \quad (x + I_1, \ldots, x + I_n) \end{aligned}$$

ein Isomorphismus von Ringen.

Proof. Sei $r_1 + I_1, \cdots, r_n + I_n$ ein beliebliges Element in $\Pi_{i=1}^n R/I_i$. Chinesischer Restsatz $\Rightarrow$ $a \in R$ mit $a \equiv r_i (\text{mode } I_1), i = 1, \cdots, n$. Klar: $\overline{\varphi}(\overline{a}) = (a + I_1, \cdots, a + I_n)$ □

Die Surjektivität von φ ist dabei äquivalent zur Existenzaussage im chineschen Restsatz, die Injektivität ist äquivalent zur Eindeutigkeitsaussage.

EXAMPLE 2.24. Löse $\begin{cases} a \equiv 2 (\text{mod } 10) \\ a \equiv 4 (\text{mod } 7) \end{cases}$ in $\mathbb{Z}$.
Dazu $1 = 3 \cdot 7 - 2 \cdot 10 \Rightarrow 4 - 2 = 6 \cdot 7 - 4 \cdot 10 \Rightarrow 4 - 6 \cdot 7 = 2 - 4\dot{1}0 =: a = -38$. a kann man abändern um Vielfache von 70. Also ist 32 die kleinste positive Lösung

LEMMA 2.25.

$$\begin{aligned} R/I &\overset{\simeq}{\twoheadrightarrow} \Pi_{i=1}^n R/I_i \\ a &\longmapsto (a + I_1, \cdots, a + I_n). \end{aligned}$$

LEMMA 2.26. *Sei* $R = \mathbb{Z}$. *Seien* $m_1, \cdots, m_n \in \mathbb{N}$ *paarweise teilerfremd. Seien* $a_1, \cdots, a_n \in \mathbb{Z}$. *Dann gibt es ein ganze Zahl* a *mit*

$$a \equiv a_i \ (\text{mod } m_i), \quad i = 1, \cdots, n$$

a *ist eindeutig module* $m := m_1 \cdots m_n$

Proof. Nimm $I_i = m_i Z$. Insbesondere: Sei $\mathbb{Z} \ni m = \pm \Pi_{i=1}^n p_i^{e_i}$ die Primzahlzerlegung. Dann gilt $\mathbb{Z}/m\mathbb{Z} \simeq \Pi_{i=1}^n \mathbb{Z}/p_i^{e_i}\mathbb{Z}$, $a + m\mathbb{Z} \longmapsto (a + p_1^{e_1}\mathbb{Z}, \cdots, 1 + p_n^{e_n}\mathbb{Z})$ □

DEFINITION 2.27. Ein nullteilerfreier Ring heißt auch Integritätsbereich.

DEFINITION 2.28. Ein Element $p \in R$ heißt irreduzibel, falls $p \notin R^\times$ und keine echten Teiler hat, d.h. aus $p = ab$ folgt $a \in R^\times$ oder $b \in R^\times$.

Die irreduziblen Elemente in $\mathbb{Z}$ sind genau die Primzahlen und ihre Negativen. In beliebigen Ringen gibt es jedoch einen Unterschied zwischen den Begriffen "prim" und "irreduzibel".

DEFINITION 2.29. Ein Element $p \in R$ heißt prim oder Primelement, falls gilt:

$$p \mid ab \Longrightarrow p \mid a \text{ oder } p \mid b$$

REMARK 2.30. Falls R nullteilerfrei ist, so gilt: p prim $\Longrightarrow p$ irreduzibel.

Die Umkehrung ist im Allgemeinen falsch, gilt aber in Hauptidealringen.

Proof. Sei $p = ab \Rightarrow p \mid ab \overset{\text{etwa}}{\Rightarrow} p \mid a \Rightarrow a = pc \Rightarrow p = pcb \Rightarrow p(1-cd) = 0 \Rightarrow cd = 1 \Rightarrow b \in R^*$ □

REMARK 2.31. Achtung: Die Umkehrung ist i. A. Falsch.
Gegenbeispiel: $R = \mathbb{Z}[\sqrt{-5}] \subseteq = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}\mathbb{C}$. Es gilt: $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$. $2, 3, 1\pm\sqrt{-5}$ sind irreduzibel, aber nicht prim. Z. B.: $1\pm\sqrt{-5}$ ist irreduzibel, denn: $1+\sqrt{-5} = \alpha\beta,\ \alpha, \beta \in R$. (Sei $N : \mathbb{Z}[\sqrt{-5}] \longrightarrow \mathbb{Z},\ z = z_1 + z_2\sqrt{-5} \longmapsto z\bar{z} = z_1^2 + 5z_2^2 \in \mathbb{Z}$. Es gilt $N(\alpha\beta) = N(\alpha)N(\beta)$). $6 = N(1+\sqrt{-5}) = N(\alpha\beta) = N(\alpha)N(\beta) \Rightarrow N(\alpha) \in \{1, 2, 3, 6\}$

EXAMPLE 2.32. (i) $\mathbb{Z}, \mathbb{K}[x]$ sind Integritätbereiche.

(ii) $R[x]$ ist ein Integritätbereiche, falls R nullteilerfrei ist, denn $\begin{cases} f(x) = a_n x^n + \cdots, & a_n \neq 0 \\ g(x) = b_m x^m + \cdots, & b_m \neq 0 \end{cases} \Rightarrow$ $f(x)g(x) = a_n b_m xn + m + \cdots \neq 0$

(iii) $R[x]^\times = R^\times$, falls R nullteilerfrei.

(iv) $R = \mathbb{Z}/m\mathbb{Z}$.

LEMMA 2.33. *Sei* $a \in \mathbb{Z}$ *und* $\bar{a} = a + m\mathbb{Z} \in \mathbb{Z}/m\mathbb{Z}$.

(i) $\bar{a} \in (\mathbb{Z}/m\mathbb{Z})^\times \Leftrightarrow \mathrm{ggT}(a, m) = 1$

(ii) $\bar{a}$ *ist Nullteiler* $\Leftrightarrow \mathrm{ggT}(a, m) > 1$

Proof. (i)
- " $\Rightarrow$ " : $\exists b \in \mathbb{Z} : ab \equiv 1 (\mathrm{mod}\ m) \Rightarrow \exists c : ab = 1 + cm \Rightarrow 1 = ab - cm \Rightarrow \mathrm{ggT}(a, m) = 1$
- " $\Leftarrow$ " : Euklidischer Algorithmus $\Rightarrow \exists x, y \in \mathbb{Z} : 1 = xa + ym \Rightarrow xa \equiv 1 (\mathrm{mod}\ m)$, d.h. $\bar{a}^{-1} = \bar{x}$

(ii)
- " $\Rightarrow$ " : $\bar{a}$ Nullteiler $\Rightarrow \bar{a} \notin R^\times \Rightarrow \mathrm{ggT}(a, m) > 1$
- " $\Leftarrow$ " : Sei $d := \mathrm{ggT}(a, m)$. Dann: $a \cdot \frac{m}{d} = \frac{a}{d} \cdot m \equiv 0 (\mathrm{mod}\ m)$ bzw.$\bar{a} \cdots \overline{\left(\frac{m}{d}\right)} = \bar{0}$

□

THEOREM 2.34. *Sei* R *ein Hauptidealring. Dann gilt:* p *ist prim* $\Longleftrightarrow p$ *ist irreduzibel.*

DEFINITION 2.35. Sei R nullteilerfrei. Dann ist R ein ZPE-Ring (oder faktoriell), falls gilt:

(i) Jedes Element $a \in R\backslash\{0\}, a \notin R^\times$, kann man als Produkt

$$a = c_1 \cdots c_n \text{ mit irreduziblen } c_i \in R$$

schreiben.

(ii) (Eindeutigkeit) Falls $a = c_1 \cdots c_n = d_1 \cdots d_m$ mit irreduziblen Elementen c_i und d_j, so gilt $n = m$ und (bis auf Numerierung) $c_i \sim d_i$.

THEOREM 2.36. *Jeder nullteilerfreie euklidische Ring ist ein HIR.*

Proof. Wie bei $\mathbb{Z}$. □

LEMMA 2.37. *Sei* R *ein Hauptidealring und* $a_1, \cdots, a_n \in R$ *Sei* $(a_1, \cdots, a_n) := (a_1) + \cdots + (a_n) \lhd R$. *Dann gilt:* $(a_1, \cdots, a_n) = (d) \Leftrightarrow d = \mathrm{ggT}(a_1, \cdots, a_n)$. *Insbesondere existiertin HIR ein ggT.*

Proof.
- " $\Rightarrow$ ": $(a_i) \subseteq (d) \Leftrightarrow d \mid a_i,\ i = 1, \cdots, n$ Sei $d' \mid a_i,\ i = 1, \cdots, n \Rightarrow (a_i) \subseteq (a_1) \subseteq (d') \Rightarrow (a_1, \cdots, a_n) = (d) \subseteq (d') \Rightarrow d' \mid d$.

- " $\Leftarrow$ ": $d \mid a_i,\ i = 1, \cdots, n \Leftrightarrow (a_i) \subseteq (d) \Rightarrow (a_1, \cdots, a_n) \subseteq (d)$ Sei $(a_1, \cdots, a_n) = (c) \Rightarrow c \mid a_i,\ i = 1, \cdots, n \Rightarrow c \mid d \Leftrightarrow (d) \subseteq (c) = (a_1, \cdots, a_n)$

□

Theorem 2.38. *Jeder Hauptidealring ist ein ZPE-Ring.*

Proof.

- " $\Rightarrow$ " : breits gezeigt.
- " $\Leftarrow$ " : Sei $p \mid ab,\ p \nmid a$. Z.z.$p \mid b$.
  Betrachte $(p) + (b) = (c), c \in R \Rightarrow (p) \subseteq (c) \Leftrightarrow c \mid p \Rightarrow c \in R^\times$ oder $c \sim p$

□

Grundlegend für den Beweis dieses Satzes ist das

Lemma 2.39. *Sei* R *ein Hauptidealring. Dann wird jede aufsteigende Kette*

$$(a_0) \subseteq (a_1) \subseteq (a_2) \subseteq \ldots$$

von Idealen in R *stationär, d.h. es gibt* $n \in \mathbb{N}$*, so daß* $(a_i) = (a_n)$ *für alle* $i \geqslant n$.

Proof. Sei $J := \bigcup_{i=1}^{\infty}(a_i)$. Dann ist J ein Ideal! Also $J = (a)$. Sei n so, daß$a \in (a_n)$. Dann gilt : $(a_{n+l}) = (a_n), \forall l \geqslant 0$ □

2.2 Lineare Kongruenzen

Theorem 2.40 (Lineare Kongruenz). *Eine lineare Kongruenz bezeichnet in der Zahlentheorie eine diophantische Gleichung in Form der Kongruenz*

$$ax = b \mod m$$

Sei

$$\mathrm{ggT}(a, m) = d$$

Diese Kongruenz hat genau dann Lösungen, wenn d *ein Teiler von* b *ist:*

$$d|b$$

Sei r *eine spezielle Lösung, dann besteht die Lösungsmenge aus* d *verschiedenen Kongruenzklassen. Die Lösungen* x *besitzen dann die Darstellung*

$$x = r + t \cdot \frac{m}{d}, \ \ t \in \mathbb{Z}$$

Theorem 2.41 (Chinesischer Restklassesatz). *Schon*

2.3 Einheiten in $\mathbb{Z}/(n)$

$$\bar{a} \in (\mathbb{Z}/(n))^{\times} \Leftrightarrow \exists \bar{x} \in (\mathbb{Z}/(n))^{\times} \quad \text{mit} \quad \bar{a} \cdot \bar{x} = \bar{1}, \text{d.h. } ax = 1 \mod n$$

i.e. $(\mathbb{Z}/(n))^{\times} = \{\bar{a} \in (\mathbb{Z}/(n) \mid 0 < a < n \wedge a \text{ ist teilerfremd zu } n\}$

Remark 2.42. $m_1, \cdots, m_s$ pairwise relatively prime natural number. $m = m_1 \cdots m_s \Rightarrow (\mathbb{Z}/(m))^{\times} = (\mathbb{Z}/(m_1))^{\times} \times \cdots \times (\mathbb{Z}/(m_s))^{\times}$

Definition 2.43 (Euler φ-function). For $n \in \mathbb{Z}^+$ let $\phi(n)$ be the number of positive integers $a \leqslant n$ with a relatively prime to n, i.e. $(a, n) = 1$. (i.e. $\varphi(n) = \left|(\mathbb{Z}/(n))^{\times}\right|$)

Proposition 2.44. *Basic proposition of Euler φ-function:*

(i) $m_1, \cdots, m_s \in \mathbb{N}$ *pairwise relatively prim* $\Rightarrow \varphi(m_1 \cdot \cdots \cdot m_s) = \varphi(m_1) \cdot \cdots \cdot \varphi(m_s)$

(ii) $p \in \mathbb{P} \Rightarrow \varphi(p^n) = p^{n-1}(p-1)$

(iii) $n \in \mathbb{N} \Rightarrow \prod_{p|n \wedge p \in \mathbb{P}}(1 - \frac{1}{p})$

Proof. TODO:ZAI SHUO □

Definition 2.45 (Primitive root modul p). A number g is a primitive root modulo n if every number a coprime to n is congruent to a power of g modulo n.

Remark 2.46. i.e. $\{1, g, g^2, \cdots, g^[p-2]\} = \mathbb{F}_p^+$.

Theorem 2.47. $(\mathbb{F}_p)^+$ *is cyclic.*
In particular, there is a isomorphism $g : \mathbb{Z}/(p-1) \longrightarrow (\mathbb{Z}/(p))^+)$, $m \longmapsto g^m$ *for* g.