1 Script zur Vorlesung: Algebra 1 (WiSe2020-2021)

Prof. Dr. Salma Kuhlmann

Kurze Einleitung:
Für die Vorlesung Algebra 1 (B3) haben wir vier Kapitel vorgesehen. Das erste Teil besteht aus Kapitel 1 (Ringe) und Kapitel 2 (Körpererweiterungen), das zweite Teil aus Kapitel 3 (Gruppen) und Kapitel 4 (Einführung in die Galoistheorie). In der B4 Vorlesung (Algebra 2 und algebraische Zahlentheorie) werden wir unser Studium von Galois Erweiterungen fortsetzen und vertiefen. Das Vorlesungskalender ist zur Orientierung, und enthält eine voraussichtliche Themenplanung.

Kapitel 1

RINGE

In diesem Kapitel werden wir folgende Ringe und Ringkonstruktionen untersuchen (im Stichwort): Faktorringe, Ringe von Brüchen, Lokalisierungen, Euklidische Ringe, Hauptideal Ringe, Faktorielle Ringe, Polynomringe.
In Skript 1, werden wir zunächst einige Begriffe (die wir schon in Lineare Algebra 1 und 2 gesehen haben) in Erinnerung bringen. Danach werden wir Faktorringe einführen.

§ 1 Erinnerungen

Definition 1.1.
Ein Tripel $(R, +, \cdot)$ ist ein *Ring*, falls R ist eine nichtleere Menge und $+, \cdot$ sind Verknüpfungen auf R so dass: :

- $(R, +)$ ist eine abelsche Gruppe mit neutralem Element $0 \in R$
- Die Verknüpfung $\cdot$ ist assoziativ
- die Distributivitätsgesetze gelten:

Links: $x \cdot (y + z) = (x \cdot y) + (x \cdot z) \ \forall x, y, z \in R$ und

Rechts: $(y + z) \cdot x = (y \cdot x) + (z \cdot x) \ \forall x, y, z \in R$

Definition 1.2.
Ein Ring $(R, +, \cdot)$ ist
(i) *kommutativ* falls $\forall x, y \in R : x \cdot y = y \cdot x$.
(ii) Ein *Ring mit Eins* wenn es existiert $1 \in R$ $(1 \neq 0)$ so dass $\forall x \in R : x \cdot 1 = 1 \cdot x = x$.

In dieser Vorlesung werden wir kommutative Ringe studieren.

Definition 1.3. Sei R ein kommutativer Ring mit 1.

(1) $a \neq 0; a \in R$ ist ein *Nullteiler*, wenn es $b \neq 0; b \in R$ gibt mit $ab = 0$.

(2) R ist ein *Integerring* oder *Integritätsbereich*, wenn er keine Nullteiler hat.

(3) $u \in R$ ist eine *Einheit*, wenn es ein $v \in R$ gibt mit $uv = 1$.

Notation: $R^\times :=$ Menge der Einheiten von R.

Die folgende Begriffe und Beipiele haben wir in LA I und/oder II schon studiert, wir wiederholen die Aussagen, jedoch nicht die Beweise.

Proposition 1.4.
$R^\times$ ist eine multiplikative Gruppe.

Beispiel 1.5.
Wir bezeichnen $\mathbb{Z}_n^\times$ mit $U(n)$

Es gilt: $a \in U(n) \Leftrightarrow \text{ggT}\ (a, n) = 1$.

Die Euler φ-Funktion $\varphi : \mathbb{N} \to \mathbb{N}$ wird so definiert: $\varphi(n) := \mid U(n) \mid$.

Siehe Übungsblatt für eine ausführliche Ausarbeitung der Eigenschaften von φ:

(1) $\varphi(p^v) = p^v - p^{v-1}$ für p Primzahl und $v \in \mathbb{N}$

(2) φ ist eine multiplikative arithmetische Funktion i.e. $\varphi(ab) = \varphi(a)\varphi(b)$, wenn $\text{ggT}\ (a, b) = 1$.

Definition 1.6.

(1) $S \subseteq R$ ist ein *Teilring*, wenn $S \neq \varnothing; a, b \in S \Rightarrow a - b \in S$ und $ab \in S$.

(2) Seien R, S kommutative Ringe (mit 1_R und 1_S).
Eine Abbildung $\varphi : R \to S$ ist ein *Ringhomomorphismus*, wenn
$\varphi(1_R) = 1_S, \varphi(a + b) = \varphi(a) + \varphi(b), \varphi(ab) = \varphi(a)\varphi(b)$.

(3) Ein *Ringisomorphismus* ist ein bijektiver Ringhomomorphismus.
Notation: $\varphi : R \simeq S$ oder $R \overset{\varphi}{\simeq} S$ oder $R \simeq S$.

Notation:
$\ker \varphi := \{x \in R; \varphi(x) = 0\}$
$\text{im}\ \varphi := \{y \in S; \exists x \in R \text{ mit } \varphi(x) = y\} := \varphi(R)$.

Bemerkung 1.7.
Sei φ ein Homomorphismus: φ ist injektiv $\Leftrightarrow \ker \varphi = \{0\}$.

Beispiel 1.8.
Sei $n \in \mathbb{N}$
$a \in \mathbb{Z}; \overline{a} :=$ Rest nach Division durch n.

$$\begin{array}{rccc} \varphi: & \mathbb{Z} & \to & \mathbb{Z}_n \\ & a & \mapsto & \overline{a} \end{array}$$

ist ein Ringhomomorphismus mit $\ker\varphi = \{nz / z \in \mathbb{Z}\} := n\mathbb{Z}$

Definition 1.9.
Ein Teilring $I \subseteq R$ ist ein *Ideal*, wenn aus $r \in R$ und $x \in I$ folgt: $rx \in I$.
Notation: $I \lhd R$

Beispiel 1.10.
$I = R$ und $I = \{0\}$

Terminologie:
$I \lhd R$ und $I \neq R$ heißt *echtes Ideal*.
$I \lhd R$ und $I \neq \{0\}$ heißt *nicht triviales Ideal*.

Proposition 1.11.
Sei $\varphi : R \to S$ ein Ringhomomorphismus. Es gelten:

(1) im φ ist ein Teilring von S.

(2) $\ker\varphi$ ist ein Ideal von R.

Beweis: ÜA.

§ 2 Faktorringe

Sei $I \lhd R$. Wir definieren eine binäre Relation auf R wie folgt:
$\forall x, y \in R : x \sim y \mod I$ genau dann, wenn $x - y \in I$.

Diese ist eine Äquivalenzrelation (siehe Übungsblatt).

Notation:
(i) Für $x \in R$ bezeichnen wir mit $x + I$ die Äquivalenzklasse $[x]$ von x.
(ii) Wir bezeichnen $R/I := \{x + I \mid x \in R\}$ die Menge der *Nebenklassen von R modulo I*.

Proposition 1.12.
R/I ist ein Ring mit den Ringoperationen
$(r + I) + (s + I) := (r + s) + I$ und
$(r + I) \cdot (s + I) := (rs) + I$
für alle $r, s \in R$.

Beweis: siehe Übungsblatt.

Definition 1.13.
R/I ist der *Faktorring* "$R \mod I$".

Satz 1.14. (Isomorphiesatz für Ringe)

(1) Sei $\varphi : R \to S$ ein Ringhomomorphismus. Es gilt $R/\ker\varphi \simeq \text{im}\,\varphi$.

(2) Umgekehrt: Ist $I \lhd R$, dann ist die *kanonische Projektion*
$$\begin{array}{rccc} \pi: & R & \to & R/I \\ & r & \mapsto & r+I \end{array}$$
ein surjektiver Ringhomomorphismus mit $\ker\pi = I$.

Also sind die Ideale genau die Kerne von Ringhomomorphismen.

Beweis:
Setze $I := \ker\varphi$. Wir prüfen unmittelbar dass die Abbildung

$$\begin{array}{rccc} \Phi: & R/I & \twoheadrightarrow & \varphi(R) \\ & x+I & \mapsto & \varphi(x) \end{array}$$

wohldefiniert ist, d.h. $x + I = y + I$ impliziert $\varphi(x) = \varphi(y)$.

Es ist außerdem klar, dass Φ surjektiv und ein Ringhomomorphismus ist (ÜA).

Wir berechnen nun $\ker\Phi$:
$\Phi(x+I) = 0 \Leftrightarrow \varphi(x) = 0 \Leftrightarrow x \in \ker\varphi \Leftrightarrow x \in I \Leftrightarrow x + I = 0 + I$;
somit ist $\ker\Phi = \{0 + I\}$ (das Nullelement der Faktorring R/I).

Es folgt aus Bemerkung 1.7 dass die Abbildung auch injektiv, und damit ein Isomorphismus.

Der Beweis von (2) ist analog. Siehe Übungsblatt. □

Beispiel 1.15.
Betrachte die Abbildung in Beispiel 1.8:
$$\begin{array}{rccc} \varphi: & \mathbb{Z} & \to & \mathbb{Z}_n \\ & a & \mapsto & \overline{a} \end{array}$$
ist ein Ringhomomorphismus mit $\ker\varphi = \{nz / z \in \mathbb{Z}\} := n\mathbb{Z}$

Es folgt nun aus Satz 1.14 dass $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$

Korollar 1.16.
Sei $I \lhd R, J \lhd R$ mit $I \subseteq J$ (insbesondere $I \lhd J$). Dann ist $J/I \lhd R/I$ und $(R/I)/(J/I) \simeq R/J$.

Beweis:
Die Abbildung
$$\begin{array}{rccc} \Phi: & R/I & \twoheadrightarrow & R/J \\ & x+I & \mapsto & x+J \end{array}$$
ist ein surjektiver Ringhomomorphismus mit $\ker\Phi = J/I$. Die Behauptung folgt nun aus Satz 1.14. □