Ringisomorphismen und Einheiten

Lemma (14.10)

Seien R und S Ringe. Dann gilt

(i) $(R \times S)^\times = R^\times \times S^\times$

(ii) Ist $\phi : R \to S$ ein Isomorphismus von Ringen, dann gilt $\phi(R^\times) = S^\times$. Insbesondere sind die Einheitengruppen $R^\times$ und $S^\times$ also isomorph.

Sind $m, n \in \mathbb{N}$ teilerfremd, dann gilt auf Grund des Chinesischen Restsatzes also

$$(\mathbb{Z}/mn\mathbb{Z})^\times \quad \cong \quad (\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})^\times \quad \cong \quad (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times.$$

Existenz von Primitivwurzeln

Satz (14.13)

Sei K ein Körper und U eine endliche Untergruppe der multiplikativen Gruppe $K^\times$. Dann ist U zyklisch. Insbesondere ist die multiplikative Gruppe eines endlichen Körpers immer eine zyklische Gruppe.

Folgerung (14.14)

Ist p eine Primzahl, dann gilt $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$.

Eine Zahl $a \in \mathbb{Z}$ mit der Eigenschaft $(\mathbb{Z}/p\mathbb{Z})^\times = \langle a + p\mathbb{Z} \rangle$ wird Primitivwurzel modulo p genannt.

Lemma (14.15)

(i) Sei p eine ungerade Primzahl und $m \in \mathbb{N}$. Dann gilt $(1+p)^{p^{m-1}} \equiv 1 \bmod p^m$ und $(1+p)^{p^{m-1}} \not\equiv 1 \bmod p^{m+1}$.

(ii) Für alle $m \in \mathbb{N}$, $m \geq 2$ gilt $5^{2^{m-2}} \equiv 1 \bmod 2^m$ und $5^{2^{m-2}} \not\equiv 1 \bmod 2^{m+1}$.

Beweis von Lemma 14.15, nur (i)

zu (i) geg.: ungerade Primzahl p

Beh.: $\forall m \geq 2$: $(1+p)^{p^{m-1}} \equiv 1 \mod p^m$, $(1+p)^{p^{m-1}} \not\equiv 1 \mod p^{m+1}$

Beweis durch vollst. Ind.:

Ind.-Anf. $m = 1$: $(1+p)^{p^0} = 1+p \equiv 1 \mod p$ (offensichtlich)

$(1+p)^{p^0} = 1+p \not\equiv 1 \mod p^2$, weil p^2 kein Teiler von $(1+p)-1 = p$ ist

Ind-Schritt: $m \mapsto m+1$

Nach Ind-V. existiert ein $k \in \mathbb{Z}$ mit $(1+p)^{p^{m-1}} = 1 + kp^m$, wobei auf Grund des zweiten Bed. $p \nmid k$ gilt.

z.zg: $(1+p)^{p^m} \equiv 1 \mod p^{m+1}$, $(1+p)^{p^m} \not\equiv 1 \mod p^{m+2}$

$$(1+p)^{p^m} = \left((1+p)^{p^{m-1}}\right)^p = (1+kp^m)^p = \sum_{j=0}^{p} \binom{p}{j} k^j p^{mj}$$

$$= 1 + kp^{m+1} + \sum_{j=2}^{p} \binom{p}{j} k^j p^{mj}$$

Für $2 \le j < p$ ist $\binom{p}{j}$ durch p teilbar $\Rightarrow \binom{p}{j} k^j p^{mj}$ ist teilbar durch p^{mj+1}, wobei $mj+1 \ge 2m+1 \ge m+2$.

$\Rightarrow \binom{p}{j} k^j p^{mj}$ ist teilbar durch p^{m+2}

Für $j = p$ erhalten wir $p^{mj} = p^{mp}$ und $mp \ge 3m \ge m+2$

$\Rightarrow$ Auch der letzte Summand ist teilbar durch p^{m+2}. $\Rightarrow$

insgesamt: $(1+p)^{p^m} \equiv 1 + kp^{m+1} \mod p^{m+2}$ mit $k \nmid p$ $\Rightarrow$

$(1+p)^{p^m} \equiv 1 \mod p^{m+1}$ und $(1+p)^{p^m} \not\equiv 1 \mod p^{m+2}$ $\square$

Struktur der primen Restklassengruppen

Satz (14.16)

(i) Für jede ungerade Primzahl p und jedes $m \in \mathbb{N}$ ist $(\mathbb{Z}/p^m\mathbb{Z})^\times$ eine zyklische Gruppe der Ordnung $p^{m-1}(p-1)$.

(ii) Es gilt $(\mathbb{Z}/2\mathbb{Z})^\times = \{\bar{1}\}$ und $(\mathbb{Z}/4\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z}$.
Für alle $m \geq 3$ existiert jeweils ein Isomorphismus $(\mathbb{Z}/2^m\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{m-2}\mathbb{Z}$.

Anwendung von Satz 14.16:

Bestimmung von $(\mathbb{Z}/72\mathbb{Z})^\times$

Primfaktorzerlegung: $72 = 8 \cdot 9 = 2^3 \cdot 3^2$

$\Rightarrow (\mathbb{Z}/72\mathbb{Z})^\times \cong (\mathbb{Z}/8\mathbb{Z})^\times \times (\mathbb{Z}/9\mathbb{Z})^\times \cong$

$\llcorner$ 8, 9 teilerfremd

Satz 14.16

$\varphi(9) = 6$

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \cong$

$\llcorner$ Chin. RS für Gruppen

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong$

$(\mathbb{Z}/2\mathbb{Z})^3 \times \mathbb{Z}/3\mathbb{Z}$.

Beweis von Satz 14.16:

<u>zu (i)</u> geg: Primzahl $p \geq 3$, $m \in \mathbb{N}$, $m \geq 2$

zzg: $(\mathbb{Z}/p^m\mathbb{Z})^*$ ist zyklisch von Ordnung $\varphi(p^m) = p^{m-1}(p-1)$

<u>Beh</u>: Die Gruppe enthält ein Element $\bar{a}$ der Ordnung p^{m-1} und ein Element $\bar{b}$ der Ordnung $p-1$

Sei $\bar{a} = \bar{1} + \bar{p}$. Lemma 14.15 $\Rightarrow (1+p)^{p^{m-1}} \equiv 1 \mod p^m$ und $(1+p)^{p^{m-2}} \not\equiv 1 \mod p^m \Rightarrow \bar{a}^{p^{m-1}} = \bar{1}$ und $\bar{a}^{p^{m-2}} \neq \bar{1}$. Laut Gruppentheorie folgt daraus $\operatorname{ord}(\bar{a}) = p^{m-1}$ in der Gruppe $(\mathbb{Z}/p^m\mathbb{Z})^*$

Sei $c \in \mathbb{Z}$ eine Primitivwurzel modulo p.

($\Rightarrow$ Das Bild von c in $(\mathbb{Z}/p\mathbb{Z})^\times$ hat Ordnung $p-1$.)

Sei $\bar{c} = c + p^n\mathbb{Z} \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ und $r = \operatorname{ord}(\bar{c})$.

$\bar{c}^r = \bar{1}$ in $\mathbb{Z}/p^m\mathbb{Z} \Rightarrow c^r \equiv 1 \mod p^m$

$\Rightarrow c^r \equiv 1 \mod p \Rightarrow (c+p\mathbb{Z})^r = 1 + p\mathbb{Z}$

in $(\mathbb{Z}/p\mathbb{Z})^\times \Rightarrow (p-1) \mid r \Rightarrow \exists k \in \mathbb{Z} : r = k(p-1)$

$[\operatorname{ord}(c+p\mathbb{Z}) = p-1]$

Setzen wir $\bar{b} = \bar{c}^k$, dann gilt also $\operatorname{ord}(\bar{b}) =$

$\frac{\operatorname{ord}(\bar{c})}{k} = p-1$ ($\Rightarrow$ Beh.)

Definiere nun in $(\mathbb{Z}/p^n\mathbb{Z})^\times$ die Untergruppen

$U = \langle \bar{a} \rangle$ und $V = \langle \bar{b} \rangle$

14 · 16
$g) = 6$

<u>Beh</u>: $(\mathbb{Z}/p^n\mathbb{Z})^\times$ ist inneres direktes Produkt von U und V (Daraus folgt dann $(\mathbb{Z}/p^n\mathbb{Z})^\times \cong U \times V \cong \mathbb{Z}/p^{n-1}\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \cong \mathbb{Z}/p^{n-1}(p-1)\mathbb{Z}$.) ← Chin. RS für Gruppen

klar: U, V sind Normalteiler von $(\mathbb{Z}/p^n\mathbb{Z})^\times$ (weil die Gruppe abelsch ist) noch zu überprüfen:

(1) $U \cap V = \{\bar{1}\}$ (2) $(\mathbb{Z}/p^n\mathbb{Z})^\times = UV$

<u>zu (1)</u> folgt aus der Teilerfremdheit von $|U| = p^{n-1}$, $|V| = p-1$

<u>zu (2)</u> U, V Normalteiler $\Rightarrow UV$ Untergr. von $(\mathbb{Z}/p^n\mathbb{Z})^\times$

$U \leq UV$, $V \leq UV \overset{\text{Lagrange}}{\Rightarrow} p^{n-1}, p-1$ sind Teiler von $|UV| \Rightarrow p^{n-1}(p-1) \mid |UV| \Rightarrow |UV| \geq p^{n-1}(p-1) =$

$|(\mathbb{Z}/p^n\mathbb{Z})^*| \overset{UV\subseteq(\mathbb{Z}/p^n\mathbb{Z})^*}{\Longrightarrow} (\mathbb{Z}/p^n\mathbb{Z})^* = UV$

zu (ii) $\varphi(2) = 1 \Rightarrow (\mathbb{Z}/2\mathbb{Z})^* = \{\bar{1}\}$

$\varphi(4) = 2$, 2 Primzahl $\Rightarrow (\mathbb{Z}/4\mathbb{Z})^*$ ist zyklisch von Ordnung 2

$\Rightarrow (\mathbb{Z}/4\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z}$

Sei nun $m \in \mathbb{N}$ mit $m \geq 3$. zzg: $(\mathbb{Z}/2^m\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{m-2}\mathbb{Z}$

$-\bar{1} \neq \bar{1}$, $(-\bar{1})^2 = \bar{1}$ in $(\mathbb{Z}/2^m\mathbb{Z})^* \Rightarrow \operatorname{ord}(-\bar{1}) = 2$ in $(\mathbb{Z}/2^m\mathbb{Z})^*$

Aus Lemma 14.15 (ii) folgt außerdem, dass $\bar{5}$ in $(\mathbb{Z}/2^m\mathbb{Z})^*$ ein Element der Ordnung 2^{m-2} ist. Es genügt somit zu zeigen, dass $(\mathbb{Z}/2^m\mathbb{Z})^*$ ein inneres direktes Produkt von $U = \langle -\bar{1} \rangle$ und $V = \langle \bar{5} \rangle$.

von $U = \langle -\bar{1} \rangle$ und $V = \langle \bar{5} \rangle$.

Überprüfe dafür: (1) $U \cap V = \{\bar{1}\}$ (2) $UV = (\mathbb{Z}/2^m\mathbb{Z})^\times$

zu (1) Bereits in $(\mathbb{Z}/8\mathbb{Z})^\times$ ist $-\bar{1}$ keine Potenz von $\bar{5}$, also gilt dies erst recht in $(\mathbb{Z}/2^{m-2}\mathbb{Z})^\times$. $\Rightarrow \langle -\bar{1} \rangle \cap \langle \bar{5} \rangle = \{\bar{1}\}$.

zu (2) Zumindest gilt $UV \cong U \times V \Rightarrow |UV| = |U||V| = 2^{m-1} = |(\mathbb{Z}/2^m\mathbb{Z})^\times| \overset{UV \subseteq (\mathbb{Z}/2^m\mathbb{Z})^\times}{\Longrightarrow} (\mathbb{Z}/2^m\mathbb{Z})^\times = UV$. $\square$

Bereits in § 9 haben wir die Begriffe „Teilkörper“, „Erweiterungskörper“ und „Körpererweiterung“ eingeführt.

Definition (15.1)

Sei $L|K$ eine Körererweiterung. Ein Zwischenkörper von $L|K$ ein Teilkörper von L, der zugleich Erweiterungskörper von K ist.

Erzeugendensysteme von Teilkörpern

Satz (15.2)

Sei $\tilde{L}|K$ eine Körpererweiterung und $S \subseteq \tilde{L}$ eine Teilmenge. Dann gibt es einen eindeutig bestimmten Zwischenkörper L von $\tilde{L}|K$ mit den Eigenschaften

(i) $L \supseteq S$

(ii) Für jeden weiteren Zwischenkörper L' von $\tilde{L}|K$ mit $L' \supseteq S$ gilt $L' \supseteq L$.

Insgesamt ist L also der kleinste Zwischenkörper von $L|K$ mit der Eigenschaft $L \supseteq S$.

Wir bezeichnen den Körper L mit $K(S)$ und nennen ihn den von der Teilmenge S über K erzeugten Teilkörper von $\tilde{L}$.

Eigenschaften erzeugter Teilkörper

Proposition (15.3)

Sei $\tilde{L}|K$ eine Körpererweiterung, und seien S und T beliebige Teilmengen von $\tilde{L}$. Dann gilt

$$K(S \cup T) \quad = \quad K(S)(T).$$

Proposition (15.4)

Sei $\tilde{L}|K$ eine Körpererweiterung und $a \in \tilde{L}$. Dann gilt

$$K(a) \quad = \quad \left\{ \frac{f(a)}{g(a)} \;\middle|\; f, g \in K[x], g(a) \neq 0 \right\}.$$

Beweis von Proposition 15.3

geg.: Körpererweiterung $\tilde{L} | K$, $S, T \subseteq \tilde{L}$

Beh.: $K(S \cup T) = K(S)(T)$

Wir überprüfen, dass $M = K(S)(T)$ die definierenden Eigenschaften von $K(S \cup T)$ hat, im Einzelnen

(1) M ist Zwischenkörper von $\tilde{L} | K$

(2) $M \supseteq S \cup T$

(3) Ist L ein bel. Zwischenkörper von $\tilde{L} | K$ mit $L \supseteq S \cup T$, dann folgt $L \supseteq M$.

zu (1) Nach Def. ist $K(S)$ ein Zwischenkörper von

(2) $M \supseteq S \cup T$

(3) Ist L ein bel. Zwischenkörper von $\tilde{L}|K$

...

$\tilde{L}|K$, und $M = K(S)(T)$ ist ein Zwischenkörper von $\tilde{L}|K(S)$

$\Rightarrow M$ ist Teilkörper von $\tilde{L}$, außerdem:

$K(S)$ ist Teilkörper von M, K ist Teilkörper von $K(S)$ $\Rightarrow$

K ist Teilkörper von M insg. M ist Zwischenkörper von $\tilde{L}$

<u>zu (2)</u> Nach Def gilt $K(S) \supseteq S$, $K(S)(T) \supseteq T$

$\Rightarrow M = K(S)(T) \supseteq K(S) \cup T \supseteq S \cup T$

<u>zu (3)</u> Sei L ein Zwischenkörper von $\tilde{L}|K$ mit $L \supseteq S \cup T$.

zzg: $L \supseteq M$ Es gilt $L \supseteq S$, und L ist Zw.-körp. von

$\tilde{L}|K$. $\Rightarrow L \supseteq K(S) \Rightarrow L$ ist Zwischenkörper von $\tilde{L}|K(S)$.

außerdem $L \supseteq T \Rightarrow L \supseteq K(S)(T) \Rightarrow L \supseteq M$. $\square$

Der Grad einer Körpererweiterung

Definition (15.5)

Ist $L|K$ eine Körpererweiterung, dann definieren die beiden Abbildungen

$$+ : L \times L \to L\ ,\ (\alpha, \beta) \mapsto \alpha + \beta \quad \text{und} \quad \cdot : K \times L \to L\ ,\ (a, \alpha) \mapsto a\alpha$$

eine K-Vektorraumstruktur auf L. Dabei bezeichnet man $[L : K] = \dim_K L$ als den Grad der Körpererweiterung. Ist $[L : K]$ endlich, dann nennt man $L|K$ eine endliche Körpererweiterung.

Satz (15.6)

Seien $L|K$ und $M|L$ endliche Körpererweiterungen. Dann ist auch die Körpererweiterung $M|K$ endlich, und es gilt

$$[M : K] \quad = \quad [M : L] \cdot [L : K].$$

Beispiele für Erweiterungsgrade:

(1) $[\mathbb{C}:\mathbb{R}] = 2$, denn: $\{1, i\}$ ist eine zweielementige Basis von $\mathbb{C}$ als $\mathbb{R}$-Vektorraum

(2) Für jede Körpererweiterung $L|K$ gilt $[L:K]=1$ genau dann, wenn $L=K$ ist.

„$\Leftarrow$" leicht zu überprüfen: $\{1_K\}$ ist eine Basis von K als K-Vektorraum

$\Rightarrow [K:K] = 1 \overset{L=K}{\Longrightarrow} [L:K] = 1$

„$\Rightarrow$" Vor.: $[L:K] = 1$ $\quad 1_K \neq 0_K$

$\rightarrow \{1_K\}$ ist linear unabh. Teilmenge des K-Vektorraums L. Weil dieser Vektorraum 1-dimensional ist, ist $\{1_K\}$ eine Basis von L.
Für jedes $\alpha \in L$ gibt es also ein $a \in K$ mit $\alpha = a \cdot 1_K = a$. $\rightarrow L \subseteq K \overset{K \subseteq L}{\Longrightarrow} L = K$.

(3) Es gilt $[\mathbb{R}:\mathbb{Q}] = \infty$.

Grund: Man kann zeigen, dass in $\mathbb{R}$, aufgefasst als $\mathbb{Q}$-Vektorraum, unendliche linear unabhängige Teilmengen existieren, z.B. $\{\sqrt{p} \mid p \text{ Primzahl}\}$