Übungsstunde 9

Nachbesprechung Bonus

8.5 Inner Direct Products ($\star$) ***(8 Points)***

a) Let $\langle G; *, \widehat{\ }, e\rangle$ be a commutative group. Let H and K be subgroups of G such that

i. $G = \{h * k \mid h \in H, k \in K\}$,

ii. $H \cap K = \{e\}$.

Prove that G is isomorphic to the direct product $H \times K$. In this case, G is called the *inner* direct product of H and K.

b) Use the previous subtask to prove that $\langle \mathbb{Z}_{15}^*, \odot_{15}\rangle \simeq \mathbb{Z}_2 \times \mathbb{Z}_4$. You can use the subtask even if you have not proven it. **Do not** prove the isomorphism directly.

Isomorphe und zyklische Gruppen - Übersicht

Isomorphe Gruppen:

- $\langle \mathbb{Z}_{nm}, \oplus \rangle \simeq \langle \mathbb{Z}_n, \oplus \rangle \times \langle \mathbb{Z}_m, \oplus \rangle$, wenn gcd(n,m)=1
  Isomorphismus: $\psi: \mathbb{Z}_{nm} \to \mathbb{Z}_n \times \mathbb{Z}_m, \psi(a) = \big(R_n(a), R_m(a)\big)$
- $\langle \mathbb{Z}^*_{nm}, \odot \rangle \simeq \langle \mathbb{Z}^*_n, \odot \rangle \times \langle \mathbb{Z}^*_m, \odot \rangle$, wenn gcd(n,m)=1
- Jede zyklische Gruppe G mit $|G| = n$ ist isomorph zu $\langle \mathbb{Z}_n, \oplus \rangle$

Zyklische Gruppen:

Gruppe	Anzahl Elemente	Zyklisch?
$\langle \mathbb{Z}_n, \oplus \rangle$	n	Für alle $n \in \mathbb{N}$
$\langle \mathbb{Z}_n, \oplus \rangle \times \langle \mathbb{Z}_m, \oplus \rangle$	$n * m$	Wenn gcd(n,m)=1
$\langle \mathbb{Z}^*_n, \odot \rangle$	$\varphi(n)$	Wenn $n \in \{2,4, p^e, 2p^e\}$ für eine Primzahl $p > 2$ und $e \geq 1$
$\langle \mathbb{Z}^*_n, \odot \rangle \times \langle \mathbb{Z}^*_m, \odot \rangle$	$\varphi(n) * \varphi(m)$	Wenn gcd(n,m)=1 und $\mathbb{Z}^*_{nm}$ zyklisch
G	$\lvert G \rvert = p$	Wenn p Primzahl

Fermat

Corollary 5.14 (Fermat, Euler). *For all $m \geq 2$ and all a with $\gcd(a, m) = 1$,*

$$a^{\varphi(m)} \equiv_m 1.$$

In particular, for every prime p and every a not divisible by p,

$$a^{p-1} \equiv_p 1.$$

Aufgabe: Berechne $R_{21}(16^{14})$

Aufgabe

- Es gilt $\gcd(16, 21) = 1$
- $\varphi(21) = \varphi(7 \cdot 3) = 6 \cdot 2 = 12$
- Somit folgt aus Fermat: $16^{12} \equiv_{21} 1$ oder anders geschrieben $R_{21}(16^{12}) = 1$

$$R_{21}(16^{14}) = R_{21}(16^{12} \cdot 16^2) = R_{21}(16^2) = R_{21}((-5)^2) = R_{21}(25) = 4$$

$16 \equiv_{21} -5$

Ringe

Für ein Ring $\langle R, +, -, 0, *, 1 \rangle$ gilt

i. $\langle R, +, -, 0 \rangle$ ist kommutative Gruppe

ii. $\langle R, *, 1 \rangle$ ist Monoid

iii. $a(b + c) = (ab) + (ac)$ und $(b + c)a = (ba) + (ca)$

Der Ring ist kommutativ, wenn * kommutativ: $a * b = b * a$

Aufgabe

9.4 Non-Minimality of Ring Axioms ($\star$) ***(8 Points)***

In this exercise, you prove the remark in Chapter 5, Footnote 20 of the lecture notes.
Consider an algebra $\langle R; +, -, 0, \cdot, 1\rangle$ such that

i) $\langle R; +, -, 0\rangle$ is a group.

ii) $\langle R; \cdot, 1\rangle$ is a monoid.

iii) $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$ for all $a, b, c, \in R$.

Prove that such an algebra satisfies Definition 5.18 in the lecture notes. Each step should consist of one or more applications of the given axioms, and the axioms used should be made explicit.
Hint: consider $(1 + 1)(a + b)$.

Aufgabe

Wir müssen zeigen, dass + kommutativ ist. Wir betrachten zuerst den Hinweis.

Sei $a, b \in R$

$$(1+1)(a+b) = (1+1)a + (1+1)b \quad \text{(iii)}$$
$$= 1a + 1a + 1b + 1b \quad \text{(iii)}$$
$$= a + a + b + b \quad \text{(ii, 1 n.e.)}$$

→ Wir haben hier zwei Möglichkeiten $(1+1)(a+b)$ mit Distributivität umzuformen. Wir betrachten beide Möglichkeiten und kommen auf zwei Ergebnisse.

$$(1+1)(a+b) = 1(a+b) + 1(a+b) \quad \text{(iii)}$$
$$= 1a + 1b + 1a + 1b \quad \text{(iii)}$$
$$= a + b + a + b \quad \text{(ii, 1 n.e.)}$$

$$(1+1)(a+b) = (1+1)(a+b)$$
$$\Leftrightarrow\ a+a+b+b = a+b+a+b$$
$$\Leftrightarrow\ a+a+b+b+(-b) = a+b+a+b+(-b) \quad (+(-b) \text{ rechts})$$
$$\Leftrightarrow\ a+a+b = a+b+a \quad \text{(i, Assoziativität und Inverse)}$$
$$\Leftrightarrow\ (-a)+a+a+b = (-a)+a+b+a \quad (-(-a) \text{ links})$$
$$\Leftrightarrow\ a+b = b+a \quad \text{(i, Assoziativität und Inverse)}$$

$a+b = b+a$ Kommutativität

Aufgabe

a) Let $\langle R; +, -, 0, \cdot, 1 \rangle$ be a ring such that for any $a, b \in R$ we have

$$a^2 b = aba.$$

Prove that R is commutative.

Hint: Consider the expression $(x+1)^2 y$.

Aufgabe

Wir müssen zeigen: $x \cdot y = y \cdot x$ für alle $x, y \in \mathbb{R}$

$$
\begin{aligned}
(x+1)^2 y &= (x+1)\cdot(x+1)\cdot y \\
&= (x(x+1)+1(x+1))\cdot y && \text{(distr.)} \\
&= (x^2 + x + x + 1)\cdot y && \text{(distr., 1 n.e.)} \\
&= x^2 y + xy + xy + y && \text{(distr., 1 n.e.)}
\end{aligned}
$$

$$
\begin{aligned}
(x+1)^2 y &: (x+1)\,y\,(x+1) \\
&= (xy + y)(x+1) && \text{(distr., 1 n.e)} \\
&= (xy+y)x + (xy+y) && \text{(distr., 1 n.e)} \\
&= xyx + yx + xy + y && \text{(distr.)} \\
&= x^2 y + yx + xy + y && \text{(Annahme)}
\end{aligned}
$$

Somit gilt:

$$
\begin{aligned}
& x^2 y + xy + xy + y = x^2 y + yx + xy + y \\
\Rightarrow\ & -(x^2 y) + x^2 y + xy + xy + y = -(x^2 y) + x^2 y + yx + xy + y && (-(x^2y) \text{ auf der linken Seite}) \\
\Rightarrow\ & xy + xy + y = yx + xy + y && (- \text{ inverse}) \\
\Rightarrow\ & xy + xy + y - (xy + y) = yx + xy + y - (xy + y) && (-(xy+y) \text{ auf der rechten Seite}) \\
\Rightarrow\ & xy = yx && (- \text{ inverse})
\end{aligned}
$$

Einheiten und Nullteiler

- $a \in R \backslash \{0\}$ ist Einheit, wenn $a * b = b * a = 1$ für ein $b \in R$
- R^* ist die Menge der Einheiten von R
- $a \in R \backslash \{0\}$ ist Nullteiler, wenn $a * b = 0$ für ein $b \in R \backslash \{0\}$

- Für **endliche** Gruppen gilt: Jedes Element ist entweder Einheit, Nullteiler oder 0.

- Integral Domain: Kommutativer Ring ohne Nullteiler

Aufgabe

Finde alle Einheiten und Nullteiler von $\mathbb{Z}_{10}$

Aufgabe

Wir erinnern uns an die multiplikative Inverse: $ax \equiv_n 1$ existiert genau dann wenn $\gcd(a,n)$.
Somit für alle $a \in \mathbb{Z}_{10}$ mit $\gcd(a,10)=1$
Die Einheiten sind also: $\mathbb{Z}_{10}^* = \{1,3,7,9\}$
Wir können dies überprüfen: $1 \cdot 1 = 1$

$3 \cdot 7 \equiv_{10} 1$

$7 \cdot 3 \equiv_{10} 1$

$9 \cdot 9 \equiv_{10} 1$

Der Rest der Menge sind dann die Nullteiler: $2,4,5,6,8$
Auch die können wir überprüfen: $2 \cdot 5 \equiv_{10} 0$

$4 \cdot 5 \equiv_{10} 0$

$5 \cdot 2 \equiv_{10} 0$

$6 \cdot 5 \equiv_{10} 0$

$8 \cdot 5 \equiv_{10} 0$

Polynome in Ringen

Für ein kommutativen Ring R ist R[x] der kommutative Ring der Polynome über R.

Polynome in Ringen

Beispiel: Wir betrachten $\mathbb{Z}_4[x]$:

- Dann gilt z.B.:

  $3x^5 + 2x + 1 \in \mathbb{Z}_4[x]$ → Grad 5

  $x^2 + 3x \in \mathbb{Z}_4[x]$ → Grad 2

  $4x^3 + 2x \notin \mathbb{Z}_4[x]$, da $4 \notin \mathbb{Z}_4$

- Addition:

  $(3x^5 + 2x^3 + x^2 + 1) + (1x^5 + 2x^4 + 3x^3 + 2) = 2x^4 + x^3 + x^2 + 3$

  ← Wir addieren wie normale Polynome, jedoch immer mod 4, da wir in $\mathbb{Z}_4[x]$ sind!

- Subtraktion:

  $(2x^4 + x^2 + 3) - (3x^4 + x^3 + x^2 + 2) = 3x^4 + 3x^3 + 1$

- Multiplikation:

  $(3x^2 + 2x + 1) \cdot (2x^2 + 2) = 2x^4 + 2x^2 + 2x^2 + 2 = 2x^4 + 2$

Körper

Ein Körper F ist ein kommutativer Ring mit $F^* = F\backslash\{0\}$

Oder: Ein Körper ist $\langle F, +, -, 0, *, ^{-1}, 1\rangle$ mit

$\langle F, +, -, 0\rangle$ ist abelsche Gruppe

$\langle F, *, ^{-1}, 1\rangle$ ist abelsche Gruppe

$\mathbb{Z}_p$ ist ein Körper genau dann wenn p prim. Wir schreiben dann auch GF(p).