Klausur Algebra I von 9.02.09

- Alle Aussagen sind zu begründen.
- Jede Lösung ist auf einem gesonderten Blatt abzugeben, welches mit Namen und Matrikelnummer zu versehen ist. Den Aufgabenzettel können Sie behalten.

Viel Erfolg !

1. Aufgabe: Gruppen

Seien G eine endliche Gruppe und

$$U, V \subseteq G$$

zwei Untergruppen. Zeigen Sie, es gilt

$$\#\, UV \bullet \#U\bigcap V = \#U \bullet \#\, V.$$

Hinweis. Zeigen Sie, das Produkt definiert eine Abbildung

$$\varphi: U \times V \longrightarrow U \bullet V$$

deren Fasern $\varphi^{-1}(x)$ alle aus derselben Anzahl von Elementen bestehen.

2. Aufgabe: Ringe

Seien A ein kommutativer Ring mit 1 und $I, J \subseteq A$ zwei Ideale mit

$$I + J = A.$$

Zeigen Sie, der Faktorring $A/I\bigcap J$ ist isomorph zum direkten Produkt

$$A/I \times A/J$$

der Ringe A/I und A/J (mit den koordinatenweisen Operationen $(x,y)+(x',y') = (x+x',y+y')$ und $(x,y)(x',y') = (xx', yy')$).

.

3. Aufgabe: endliche Körper

Seien p eine Primzahl, n eine natürliche Zahl und $q = p^n$. Beweisen Sie die folgenden Aussagen.

(a) Die Frobenius-Abbildung

$$F: \mathbb{F}_q \longrightarrow \mathbb{F}_q\,,\ x \mapsto x^p\,,$$

ist ein $\mathbb{F}_p$-Automorphismus von $\mathbb{F}_q$.

(b) Die Galois-Gruppe $G(\mathbb{F}_q/\mathbb{F}_p)$ ist die vom Frobenius-Automorphismus F erzeugte zyklische Gruppe.

Zu 1.

Falls alle Fasern von φ aus derselben Anzahl von Elementen bestehen, gilt

$$\begin{aligned}\#\, U \bullet \#\, V = \#\, U \times V &= \sum_{x \in UV} \#\, \varphi^{-1}(x) \\ &= \#\, \varphi^{-1}(e) \bullet \text{Anzahl der Fasern} \\ &= \#\, \varphi(e) \bullet \#\, UV\end{aligned}$$

und

$$\begin{aligned}\#\, \varphi(e) &= \#\, \{(u,v) \in U \times V \mid uv = e\} \\ &= \#\, \{(u,u^{-1}) \mid u \in U,\ u^{-1} \in V\}\end{aligned}$$

$= \#\{(u,u^{-1}) \mid u \in U \cap V\}$

$= \# U \cap V.$

Es reicht also, tatsächlich die Aussage über die Anzahl der Faserelemente zu beweisen. Für $u \in U$ und $v \in V$ gilt

$$\begin{aligned}\varphi^{-1}(uv) &= \{(x,y) \in U \times V \mid xy = uv\}\\ &= \{(x,y) \in U \times V \mid x^{-1}u = yv^{-1} =: z \in U \cap V\}\\ &= \{(x,y) \mid x = uz^{-1},\ y = zv,\ z \in U \cap V\}\\ &= \{(uz^{-1}, zv) \mid z \in U \cap V\}.\end{aligned}$$

Mit anderen Worten, die Abbildung

$$U \cap V \longrightarrow \varphi^{-1}(uv),\ z \mapsto (uz^{-1}, zv),$$

ist surjektiv. Wegen $z = (zv)v^{-1}$ ist sie außerdem injektiv. Also besteht

$$\varphi^{-1}(uv)$$

aus $\# U \cap V$ Elementen, und diese Anzahl ist unabhängig von u und v.

Zu 2.

Der Ring-Homomorphismus

$$A \longrightarrow A/I \times A/J,\ a \mapsto (a \bmod I,\ a \bmod J),$$

hat den Kern $I \cap J$, induziert also einen injektiven Ring-Homomorphismus

$$\varphi: A/I \cap J \longrightarrow A/I \times A/J,\ a \bmod I \cap J \mapsto (a \bmod I,\ b \bmod J).$$

Es reicht zu zeigen, dieser ist surjektiv.
Sei

$$(a \bmod I,\ b \bmod J) \in A/I \times B/J$$

ein Element aus dem Bild-Ring. Wir haben ein Element $c \in A$ zu finden mit

$$c \bmod I = a \bmod I \text{ und } c \bmod J = b \bmod J,$$

Wegen $I + J = A$ gibt es Elemente

$$u \in I \text{ und } v \in J \text{ mit } u + v = 1.$$

Wir setzen

$$c = av + bu.$$

Dann gilt

$$\begin{aligned}c \bmod I &= av \bmod I && \text{(wegen } u \in I)\\ &= a(u+v) \bmod I && \text{(wegen } u \in I)\\ &= a \bmod I && \text{(wegen } u+v = 1)\end{aligned}$$

Analog zeigt man

$$c \bmod J = b \bmod J.$$

Zu 3 (a).

Für $x, y \in \mathbb{F}_q$ gilt

$$F(x + y) = (x + y)^p = x^p + y^p = F(x) + F(y)$$

$$F(xy) = (xy)^p = x^p \cdot y^p = F(x)F(y).$$

Also ist F ein Ring-Homomorphismus. Für $x \in \mathbb{F}_p$ gilt nach dem kleinen Satz von Fermat

$$F(x) = x^p = x.$$

Also ist F ein $\mathbb{F}_p$-Homomorphismus und als solcher injektiv. Da $\mathbb{F}_q$ endlich ist, muß dann aber F sogar bijektiv sein, d.h. F ist ein $\mathbb{F}_p$-Automorphismus.

Zu 3 (b).

Weil $\mathbb{F}_q/\mathbb{F}_p$ eine Galois-Erweiterung ist, gilt

$$\#\, G(\mathbb{F}_q/\mathbb{F}_p) = [\mathbb{F}_q:\mathbb{F}_p] = n.$$

Es reicht also zu zeigen, F hat die Ordnung n. Als Element der Gruppe $G(\mathbb{F}_q/\mathbb{F}_p)$ ist die Ordnung von F ein Teiler von n. Es reicht also zu zeigen,

$$F^i \neq \mathrm{Id} \text{ für } i = 1,...,n-1.$$

Dazu reicht es ein Element $x \in \mathbb{F}_q$ zu finden mit

$$F^i(x) \neq x \text{ für } i = 1,...,n-1$$

d.h. mit

$$x^{p^i} \neq x \text{ für } i = 1,..., n-1,$$

d.h. ein Element $x \in \mathbb{F}_q^*$

$$x^{p^i - 1} \neq 1 \text{ für } i = 1,..., n-1,$$

Dazu wiederum reicht es, eine (q-1)-te primitive Einheitswurzel in $\mathbb{F}_q^*$ zu finden. Eine solche gibt es aber, wegen

$$\#\, \mathbb{F}_q^* = q-1$$

und weil die multiplikative Gruppe eines endlichen Körpers zyklisch ist.