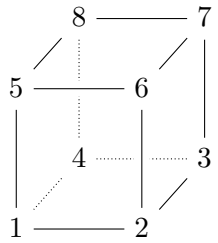
Universität Ulm

Prof. Dr. S. Wewers
WS 2013/2014

Lösungen Elemente der Algebra: Probeklausur

A1. Die Eckpunkte eines Würfels seien wie in der Abbildung nummeriert. Diese Nummerierung



führt zu einem injektiven Gruppenhomomorphismus $\varphi\colon \mathbb{W} \to S_8$.

(a) Ist die Permutation $\sigma = (1\ 2\ 3\ 4)$ ein Element von $\varphi(\mathbb{W})$? (2)

Lösung: Nein. Eine Permutation, die die obere Seite des Würfels festhält, muss die Identität sein, es ist aber σ nicht die Identität.

(b) Bestimmen Sie ein Element der Ordnung 4 in $\varphi(\mathbb{W})$. (Sie müssen nicht argumentieren, warum das von Ihnen gewählte Element in $\varphi(\mathbb{W})$ liegt.) (2)

Lösung: Ein solches Element ist $(1\ 2\ 3\ 4)(5\ 6\ 7\ 8)$.

(c) Bestimmen Sie ein Element der Ordnung 3 in $\varphi(\mathbb{W})$. (Sie müssen nicht argumentieren, warum das von Ihnen gewählte Element in $\varphi(\mathbb{W})$ liegt.) (2)

Lösung: Ein solches Element ist $(1\ 6\ 8)(2\ 7\ 4)$.

(d) Beschreiben Sie geometrisch, wie die Elemente der Ordnung 4 in $\mathbb{W}$ aussehen. Wie viele Elemente der Ordnung 4 besitzt $\mathbb{W}$ demnach? (2)

Lösung: Die Elemente der Ordnung 4 sind die Rotationen um 90 Grad um die Achse die durch zwei gegenüberliegende Seitenmittelpunkte geht. Da es drei solcher Achsen gibt und jeweils die Rotation um ± 90 Grad Ordnung 4 hat, gibt es 6 solche Elemente.

A2. Sei G eine endliche Gruppe. Zeigen oder widerlegen Sie folgende Aussagen.

(a) Seien $\sigma, \tau \in G$ konjugiert. Dann gilt $\operatorname{ord}(\sigma) = \operatorname{ord}(\tau)$. (3)

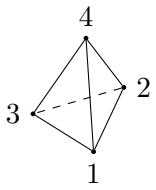
Lösung: Nach Vorraussetzung gibt es $\varrho \in G$ mit $\varrho\sigma\varrho^{-1} = \tau$. Sei $n = \operatorname{ord}(\sigma)$. Dann ist $\tau^n = (\varrho\sigma\varrho^{-1})^n = \varrho\sigma^n\varrho^{-1} = \varrho\varrho^{-1} = e$ und also $\operatorname{ord}(\tau) \leq \operatorname{ord}(\sigma)$. Vertauscht man die Rollen von τ und σ in diesem Argument, erhält man $\operatorname{ord}(\sigma) \leq \operatorname{ord}(\tau)$ und also $\operatorname{ord}(\tau) = \operatorname{ord}(\sigma)$.

(b) Seien $\sigma, \tau \in G$. Dann gilt (3)

$$\operatorname{ord}(\sigma\tau) = \operatorname{kgV}(\operatorname{ord}(\sigma), \operatorname{ord}(\tau)).$$

Lösung: Die Aussage ist falsch. Sei D_5 erzeugt von σ und τ wobei σ Ordnung fünf, τ Ordnung zwei habe. Dann hätte nach obiger Formel $\sigma\tau$ Ordnung zehn; dann wäre aber D_5 zyklisch, da es nur 10 Elemente besitzt.

A3. Auf wie viele Arten kann man die Seiten eines Tetraeders mit den Farben Grün und Rot färben? (6)



Lösung: Sei $G \subseteq S_4$ die Symmetriegruppe des Tetraeders in der Abbildung. Sei $X := \{\{1,2,3,4\} \to \{1,2\}\}$. Es wirkt G auf X vermittels $(\sigma \cdot f)(i) = f(\sigma^{-1}(i))$. Es ist $|X^e| = 16$. Für die drei Elemente in G mit Ordnung zwei gilt $|X^g| = 4$. Für die acht Elemente in G mit Ordnung drei gilt $|X^g| = 4$. Nach dem Burnside-Lemma ist also $|X/G| = \frac{1}{12}(16 + 3 \cdot 4 + 8 \cdot 4) = 5$.

A4. Bestimmen Sie im euklidischen Ring R den größten gemeinsamen Teiler der Elemente a und b. Finden Sie außerdem Elemente $s, t \in R$ mit $\mathrm{ggT}(a,b) = sa + tb$.

(a) $R = \mathbb{Z}$, $a = 91$, $b = 14$ (3)

Lösung: Es ist $\mathrm{ggT}(a,b) = 7 = 91 - 6 \cdot 14$.

(b) $R = \mathbb{F}_2[x]$, $a = x^3 + x^2 + x + 1$, $b = x^2 + x$ (3)

Lösung: Division mit Rest ergibt: $x^3+x^2+x+1 = x(x^2+x)+x+1$, $x^2+x = x(x+1)$. Somit ist $\mathrm{ggT}(a,b) = x + 1 = a + x \cdot b$.

A5. Sei R ein kommutativer Ring[1]. Sei (6)

$$I := \{a \in R : \text{ es existiert ein } n \in \mathbb{N} \text{ mit } a^n = 0\}.$$

Zeigen Sie, dass I ein Ideal von R ist.

Lösung: Sei $a, b \in I$. Dann gibt es n, m mit $a^n = 0 = b^m$. Es ist $(a+b)^{n+m} = \sum_k \binom{n+m}{k} a^k b^{n+m-k} = 0$, denn in jedem Summand ist der Exponent von a größer oder gleich n oder der Exponent von b größer oder gleich m. Damit ist $a + b \in I$. Insgesamt ist also $(I, +)$ eine abelsche Gruppe.

Sei nun $a \in I, r \in R$. Dann gibt es n mit $a^n = 0$. Es ist also $(ra)^n = r^n a^n = 0$ und somit ist $ra \in I$.

Dies zeigt, dass I ein Ideal ist.

A6. Sei $f = x^3 + x^2 + x - 1 \in \mathbb{F}_3[x]$ irreduzibel. Sei $\alpha \in \mathbb{F}_{27}$ eine Nullstelle von f. Es ist also $\mathbb{F}_{27} = \mathbb{F}_3[\alpha]$.

(a) Bestimmen Sie jeweils das Minimalpolynom von α^2, α^9 und α^{27} über $\mathbb{F}_3$. (4)

Lösung: Sei $\beta := \alpha^2$. Es gilt $\alpha^3 = -\alpha^2 - \alpha + 1$, $\alpha^4 = -\alpha^3 - \alpha^2 + \alpha = -\alpha - 1$, $\alpha^5 = -\alpha^2 - \alpha$, $\alpha^6 = -\alpha^3 - \alpha^2 = \alpha - 1$. Somit ist $\beta^3 + \beta^2 - 1 = 0$. Es ist also $g(x) = x^3 + x^2 - 1$ das Minimalpolynom von α^2, da es irreduzibel ist, da es keine Nullstellen in $\mathbb{F}_3$ hat.

Sei nun $g(x) \in \mathbb{F}_3[x]$ das Minimalpolynom von α^9. Dann ist $g(\alpha^9) = 0$. Über $\mathbb{F}_3$ gilt jedoch, dass $g(x^9) = g(x)^9$. Somit ist auch $g(\alpha) = 0$. Damit ist $g = f$.

Das gleiche Argument funktioniert auch für α^{27}. Oder man verwendet, dass $\alpha^{27} = \alpha$, da die Ordnung von α die Zahl 26 teilt; wieder ist das Minimalpolynom von α^{27} das Polynom f.

(b) Gibt es ein Element $\beta \in \mathbb{F}_3[\alpha]$ mit $\mathbb{F}_3[\beta] = \mathbb{F}_9$? Falls ja, bestimmen Sie ein solches (3)

[1]Die Aussage ist falsch, wenn man nicht fordert, dass R kommutativ ist. Im Rahmen der Vorlesung war das Wort *Ring* gleichbedeutend mit *kommutativer Ring*; und so sollte auch diese Aufgabe verstanden werden.

Element.

Lösung: Nein. Denn 3, der Exponent in $27 = 3^3$, wird nicht von 2, dem Exponenten in $9 = 3^2$, geteilt.

Oder elementarer: Es gilt $\beta \in \mathbb{F}_9^\times$ und $\beta \in \mathbb{F}_{27}^\times$. Demnach teilt die Ordnung von β die Zahlen 8 und 26. Somit hätte β Ordnung 1 oder 2. Hätte β Ordnung 1, dann wäre $\beta = e$ und $\mathbb{F}_3[\beta] = \mathbb{F}_3$. Hätte β Ordnung 2, dann wäre $\beta^2 - 1 = 0$. Das Minimalpolynom von β müsste also $x^2 - 1 = (x+1)(x-1)$ teilen und wäre somit ein Polynom vom Grad 1 und $\mathbb{F}_3[\beta] = \mathbb{F}_3$.

Oder (eigentlich das gleiche Argument, aber anders ausgedrückt): Die Elemente von $\mathbb{F}_{27}$ sind Nullstellen von $x^{27} - x$. Gleichzeitig wäre β Nullstelle von $x^9 - x$. Es gilt also $\beta = \beta^2 7 = (\beta^9)^3 = \beta^3$. Erneut würde das Minimalpolynom von β das Polynom $x^2 - 1 = (x+1)(x-1)$ teilen.

(c) Ist α ein Erzeuger von $(\mathbb{F}_3[\alpha])^\times$? (3)

Lösung: Ein solcher Erzeuger hätte Ordnung 26. Die Ordnung von α teilt $26 = 13 \cdot 2$. Es ist $\alpha^2 \neq 1$. Nun kann man naiv $\alpha^{13} = 1$ ausrechnen und schließt, dass $\mathrm{ord}(\alpha) \neq 26$. Etwas effizienter ist der folgende Ansatz, der verwendet, dass man bereits weiß, dass $\alpha^6 = \alpha - 1$. Es ist $\alpha^{13} = (\alpha^6)^2\alpha = (\alpha-1)^2\alpha = (\alpha^2+\alpha+1)\alpha = \alpha^3+\alpha^2+\alpha = 1$.

A7. Welche der folgenden Aussagen sind wahr, welche falsch? (Beantworten Sie die Fragen ohne Begründung. Die Lösung jeder Teilaufgabe soll also nur aus dem Wort *wahr* oder dem Wort *falsch* bestehen. Für jede richtige Lösung erhalten Sie 2 Punkte, für jede falsche Lösung werden Ihnen 2 Punkte abgezogen. Insgesamt können Sie jedoch nicht weniger als 0 Punkte erhalten.)

(a) Sei G eine endliche Gruppe mit n Elementen und $\sigma \in G$. Dann gilt $\mathrm{ord}(\sigma) | n$. (±2)

Lösung: Wahr. [Die von σ erzeugte Untergruppe hat $\mathrm{ord}(\sigma)$ Elemente. Nach dem Satz von Lagrange teilt diese Zahl $|G|$.]

(b) Sei G eine endliche zyklische Gruppe. Dann ist G abelsch. (±2)

Lösung: Wahr. [Sei G erzeugt von σ. Seien $a, b \in G$. Dann gibt es natürliche Zahlen n, m mit $a = \sigma^n, b = \sigma^m$. Es ist nun $ab = \sigma^n\sigma^m = \sigma^{n+m} = \sigma^m\sigma^n = ba$. Dies zeigt, dass G abelsch ist.]

(c) Sei R ein euklidischer Ring, $a \in R$. Für alle $b \in R$ gelte $a|b$. Dann ist $a \in \{-1, 1\}$. (±2)

Lösung: Falsch. [Ein Gegenbeispiel ist der euklidische Ring $\mathbb{Q}[x]$. Dort teilt 2 jedes Element, denn für $b \in \mathbb{Q}[x]$ gilt $b = 2(\frac{1}{2}b)$.]

(d) Sei $K = \mathbb{F}_{p^n}$ ein endlicher Körper. Gibt es in K ein $\alpha \neq 0$ mit $\alpha + \alpha = 0$, dann ist $p = 2$. (±2)

Lösung: Wahr. [Ist $p \neq 2$, dann ist 2 in $\mathbb{F}_{p^n}$ invertierbar. Gilt also $2\alpha = 0$, dann ist $\alpha = \frac{1}{2}2\alpha = 0$.]