Übungen 1 Lösungen: Algebra und Zahlentheorie

December 19, 2024

Übung 1.1. Eine endliche nichtleere Teilmenge einer Gruppe, die mit je zwei Elementen auch die Verknüpfung der beiden enthält, ist notwendig bereits eine Untergruppe.
Lösungen. Let S denote this subset of our group G, and let $x \in S$. Since S is closed under multiplication, S contains all powers of x. But S is finite, so there exists some integer n such that $x^n = 1$. We see that S contains the identity 1, and the inverse x^{n-1} of x. So indeed S is a subgroup of G.

Übung 1.2. Wieviele Untergruppen hat die additive Gruppe eines zweidimensionalen Vektorraums über dem Körper mit zwei Elementen? Wieviele Untergruppen hat die additive Gruppe eines n-dimensionalen Vektorraums über dem Körper mit zwei Elementen?
Lösungen. This group is $G = (\mathbb{Z}_2)^n$: the direct product of n copies of the cyclic group $\mathbb{Z}_2$. For k a positive integer, the number of k-dimensional subgroups of G equals the Gaussian binomial coefficient $\binom{n}{k}_2$. To prove this is a nice little exercise via counting linearly independent vectors, but unfortunately not what we asked (we slightly regret not asking this). To count the total number of subgroups of G, one must sum up all of these 2-binomial coefficients for all $0 \leq k \leq n$. As far as I know, this sum has no simple closed form description – see MathStackExchange 2379644. So just accept the answer written as a sum, and mark this question leniently. If $n = 2$ then G is the Klein four-group, which has 5 subgroups.

Übung 1.3. Man berechne den größten gemeinsamen Teiler von 3456 und 436 und eine Darstellung desselben als ganzzahlige Linearkombination unserer

beiden Zahlen.
Lösungen. $3456 = 2^7 * 3^3$, $436 = 2^2 * 109$, $ggT(3456, 436) = 4 = 325 * 436 - 41 * 3456$. The existence of such coefficients (here 325 and -41) is called Bézout's identity (they are not necessarily unique). One can compute these coefficients using the Euclidean algorithm (iteratively in reverse). Explicitly,

$$4 = 12 - 1 * 8 = 12 - 1(20 - 1 * 12) = 2 * 12 - 20 = 2(32 - 1 * 20) - 20 = ...$$

Übung 1.4. Gegeben zwei von Null verschiedene natürliche Zahlen a, b nennt man die kleinste von Null verschiedene natürliche Zahl, die sowohl ein Vielfaches von a als auch ein Vielfaches von b ist, das kleinste gemeinsame Vielfache von a und b und notiert sie $kgV(a, b)$. Man zeige in dieser Notation die Formel $kgV(a, b)ggT(a, b) = ab$.
Lösungen. There are many ways to show this. One can use the fundamental theorem of arithmetic, and uniquely write $a = \prod_p p^{\alpha_p}$ and $b = \prod_p p^{\beta_p}$, where p runs over all primes and the α_p, β_p's are non-negative integers. Then

$$ggT(a, b) = \prod_p p^{min\{\alpha_p, \beta_p\}}$$

and

$$kgV(a, b) = \prod_p p^{max\{\alpha_p, \beta_p\}}.$$

Since $min\{\alpha_p, \beta_p\} + max\{\alpha_p, \beta_p\} = \alpha_p + \beta_p$, the result follows.

Übungen 2 Lösungen: Algebra und Zahlentheorie

December 20, 2024

Übung 2.1. Haben zwei endliche Untergruppen einer Gruppe teilerfremde Kardinalitäten, so besteht ihr Schnitt nur aus dem neutralen Element.
Lösungen. Bezeichne mit $H_1, H_2 \subset G$ unsere Untergruppen. Es folgt direkt aus den Untergruppeneigenschaften, dass $H_1 \cap H_2$ auch eine Untergruppe von G ist. Sie ist insbesondere eine Untergruppe von H_1 und H_2, ist also endlich und teilt ihre Kardinalitäten. Da diese teilerfremd sind folgt $|H_1 \cap H_2| = 1$.

Übung 2.2. Man zeige, dass in der symmetrischen Gruppe $\mathcal{S}_4$ die Doppeltranspositionen zusammen mit dem neutralen Element einen Normalteiler $D \subset \mathcal{S}_4$ bilden, und konstruiere einen Isomorphismus $\mathcal{S}_4/D \xrightarrow{\sim} \mathcal{S}_3$.
Lösungen. D ist eine Untergruppe von $\mathcal{S}_4$, da das neutrale Element enthalten ist, die Doppeltranspositionen zu sich selbst invers sind und die Verknüpfung von zwei Doppeltranspositionen stets eine Doppeltransposition ergibt. Für letzteres betrachte repräsentativ

$$((12)(34))((13)(24)) = (14)(23).$$

Wir zeigen nun, dass die Untergruppe normal ist. Wir betrachten dazu die Konjugation von $(12)(34)$ mit den Erzeugern $(12), (13), (14)$ von $\mathcal{S}_4$

$$(12)((12)(34))(12)^{-1} = (12)((12)(34))(12) = (12)(34) \in D$$
$$(13)((12)(34))(13)^{-1} = (13)((12)(34))(13) = (14)(23) \in D$$
$$(14)((12)(34))(14)^{-1} = (14)((12)(34))(14) = (13)(24) \in D$$

Aus Symmetriegründen ist die Aussage hiermit gezeigt. $\mathcal{S}_4/D$ ist nun wohldefiniert, betrachte also

$$\tilde{\varphi} : \mathcal{S}_4 \to \mathcal{S}_4/D; \sigma \mapsto \sigma D.$$

Um zu zeigen, dass $\mathcal{S}_4/D \cong \mathcal{S}_3$ betrachten wir die paarweise disjunkten D-Nebenklassen (Bemerkung: Da D Normalteiler, stimmen Links- und Rechtsnebenklassen überein) in $\mathcal{S}_4$ und sehen, dass die 6 Elemente von $\mathcal{S}_4$, die die 4 festhalten aka die Elemente von $\mathcal{S}_3$, Repräsentanten bilden. Es gilt:

$$D\ id = D$$

$$D(123) = \{(123), (134), (243), (142)\}$$
$$D(132) = \{(132), (234), (124), (143)\}$$
$$D(12) = \{(12), (34), (1324), (1423)\}$$
$$D(13) = \{(13), (1234), (24), (1432)\}$$
$$D(23) = \{(23), (1342), (1243), (14)\}.$$

$\varphi : \mathcal{S}_4/D \to \mathcal{S}_3$ bildet nun jede Nebenklasse auf den entsprechenden Repräsentanten in $\mathcal{S}_3$ ab.
Wir rechnen nach, dass die Komposition $\phi := \varphi \circ \tilde{\varphi} : \mathcal{S}_4 \to \mathcal{S}_3$ ein Gruppenhomomorphismus ist. (Aus der Konstruktion folgt bereits, dass dieser surjektiv mit Kern D ist.) Aus der Auflistung unserer Nebenklassen erhalten wir für jedes $\sigma \in \mathcal{S}_4$ eine eindeutige Darstellung $\sigma = \delta \circ \tau$ mit $\delta \in D, \tau \in \mathcal{S}_3$. Es gilt

$$\begin{aligned} & \phi(\delta_1 \circ \tau_1 \circ \delta_2 \circ \tau_2) \\ = \ & \phi(\delta_1 \circ \bar{\delta}_2 \circ \tau_1 \circ \tau_2) \\ = \ & \tau_1 \circ \tau_2 \\ = \ & \phi(\delta_1 \circ \tau_1) \circ \phi(\delta_2 \circ \tau_2), \end{aligned}$$

wobei wir im ersten Schritt die Normalteilereigenschaft benutzt haben, genauer $\tau_1 \circ \delta_2 = \bar{\delta}_2 \circ \tau_1$ für ein $\bar{\delta}_2 \in D$. ϕ ist somit ein Gruppenhomomorphismus und wir sind fertig.

Übung 2.3. Gegeben ein surjektiver Gruppenhomomorphismus $\varphi : G \twoheadrightarrow \bar{G}$ und ein Normalteiler $\bar{N} \subset \bar{G}$ mit Urbild $\varphi^{-1}(\bar{N}) = N \subset G$ induziert φ einen Gruppenisomorphismus

$$\varphi : G/N \xrightarrow{\sim} \bar{G}/\bar{N}.$$

Lösungen. Da φ surjektiv ist, ist auch die durch φ induzierte, wohldefinierte Abbildung $\tilde{\varphi} : G \to \bar{G}/\bar{N}$ surjektiv. Der Kern dieser Abbildung ist ein Normalteiler. Wir zeigen, dass $ker(\tilde{\varphi}) = N$. Mit dem Isomorphiesatz erhalten

wir dann die gewünschte Aussage.
Sei also $g \in ker(\tilde{\varphi}) \Rightarrow \tilde{\varphi}(g) = e$ in $\bar{G}/\bar{N} \Rightarrow \varphi(g) \in \bar{N} \Rightarrow ker(\tilde{\varphi}) \subset \varphi^{-1}(\bar{N})$.
Die umgekehrte Inklusion ist klar.

Übung 2.4. Sei $G \supset H$ eine Gruppe mit einer Untergruppe. Ist G/H endlich, so zeige man, dass H einen Normalteiler N von G umfasst mit G/N endlich.
Lösungen. Wir wollen einen Gruppenhomomorphismus von G in eine endliche Gruppe finden, deren Kern in H enthalten ist. Sei

$$\varphi : G \to \mathcal{S}(G/H); g \mapsto \varphi(g)$$

wobei $\varphi(g) : G/H \xrightarrow{\sim} G/H; xH \mapsto gxH$. Offensichtlich ist $\mathcal{S}(G/H) \cong \mathcal{S}_n$ mit $n = [G : H]$. φ ist ein Gruppenhomomorphismus, da

$$\varphi(g_1 g_2)(xH) = g_1 g_2 xH = \varphi(g_1) \circ \varphi(g_2)(xH).$$

Zuletzt zeigen wir noch die Inklusion $ker(\varphi) \subset H$:

$$\begin{aligned} g \in ker(\varphi) &\Rightarrow \varphi(g) = id \\ &\Rightarrow xH = gxH \ \forall x \in G \\ &\Rightarrow H = x^{-1}gxH \ \forall x \in G \\ &\Rightarrow x^{-1}gxH \in H \ \forall x \in G \\ &\Rightarrow g \in H. \end{aligned}$$

Somit erfüllt $N = ker(\varphi)$ alle gewünschten Eigenschaften.

Übungsblatt 3 Lösungen: Algebra und Zahlentheorie

Übung 3.1. Man führe die Induktion zum Beweis des Chinesischen Restsatzes aus und zeige: Ist $m = q_1 \dots q_s$ ein Produkt von paarweise teilerfremden ganzen Zahlen, so liefert die offensichtliche Abbildung einen Isomorphismus

$$\frac{\mathbb{Z}}{m\mathbb{Z}} \xrightarrow{\sim} \frac{\mathbb{Z}}{q_1\mathbb{Z}} \times \dots \times \frac{\mathbb{Z}}{q_s\mathbb{Z}}$$

Lösung. Aus den Vorlesungen haben wir für $a, b \in \mathbb{Z}$ teilerfremd

$$\frac{\mathbb{Z}}{ab\mathbb{Z}} \xrightarrow{\sim} \frac{\mathbb{Z}}{a\mathbb{Z}} \times \frac{\mathbb{Z}}{b\mathbb{Z}}. \tag{1}$$

Dies gilt als Induktionsanfang.
Induktionsschritt: Wir nehmen an, dass

$$\frac{\mathbb{Z}}{q_1 \dots q_{n-1}\mathbb{Z}} \xrightarrow{\sim} \frac{\mathbb{Z}}{q_1\mathbb{Z}} \times \dots \times \frac{\mathbb{Z}}{q_{s-1}\mathbb{Z}}. \tag{2}$$

Dann setzen wir (1) mit $a = q_1 \dots q_{s-1}$, $b = q_s$ (noch teilerfremd) und (2) ein und schließen daraus, dass

$$\frac{\mathbb{Z}}{m\mathbb{Z}} \xrightarrow{\sim} \frac{\mathbb{Z}}{q_1 \dots q_{s-1}\mathbb{Z}} \times \frac{\mathbb{Z}}{q_s\mathbb{Z}} \xrightarrow{\sim} \frac{\mathbb{Z}}{q_1\mathbb{Z}} \times \dots \times \frac{\mathbb{Z}}{q_s\mathbb{Z}},$$

□

Übung 3.2. Gegeben Primzahlen $p_1, \dots, p_r$ und eine Zahl e mit

$$e \equiv 1 \ (mod \ (p_i - 1)) \ \forall i,$$

zeige man für alle $a \in \mathbb{Z}$ die Kongruenz

$$a^e \equiv a \pmod{p_1 \dots p_r}.$$

Berichtigung: Diese Aussage stimmt nicht, falls die p_i nicht verschieden sind. z.B. $p_1 = p_2 = 3$, nehmen wir $e = 3 \equiv 1 \pmod{3-1}$, dann ist $(3 + 9\mathbb{Z})^3 = 27 + 9\mathbb{Z} = 0 + 9\mathbb{Z} \neq 3 + 9\mathbb{Z}$.

Lösung. Die Aussage ist äquivalent dazu, dass $a^e = a$ für jedes $a \in R$ gilt, $R := \frac{\mathbb{Z}}{p_1 \dots p_r \mathbb{Z}}$. Nach dem Chinesischen Restsatz wissen wir, dass

$$R \cong \frac{\mathbb{Z}}{p_1\mathbb{Z}} \times \dots \times \frac{\mathbb{Z}}{p_r\mathbb{Z}} \cong \mathbb{F}_{p_1} \times \dots \times \mathbb{F}_{p_r}.$$

Deswegen dürfen wir uns nur einen Faktor anschauen. Die Aussage ist klar für $a = 0 \in \mathbb{F}_{p_i}$. Nach dem kleinen fermatschen Satz gilt es, dass $a^{p_i - 1} = 1$ für jedes $a \in \mathbb{F}_{p_i}^\times$. Deswegen

$$a^e = a^{\frac{e-1}{p_i-1} \cdot (p_i - 1) + 1} = 1^{\frac{e-1}{p_i-1}} \cdot a^1 = a. \qquad \square$$

Übung 3.3. Gibt es ein Vielfaches von 17, dessen letzte Ziffern 39 lauten? Wie rechnen Sie sowas aus?
Lösung. Wir interessieren uns nur für die letzten zwei Ziffern, also fassen wir die Zahlen modulo 100 auf. Dann wollen wir eine Zahl $n = 10a + b$, $a, b \in \{0, 1, \dots, 9\}$ derart, dass

$$n \cdot 17 \equiv 39 \pmod{100}. \tag{3}$$

$n \cdot 17 \equiv (10a + b) \cdot 17 \equiv 70a + 17b \pmod{100}$. Deswegen muss $b = 7$, also muss $39 \equiv 70a + 119 \equiv 70a + 19 \pmod{100}$. Wir können $a = 6$ wählen. Zum Überprüfen: $67 \cdot 17 = 1139$. $\square$

Übung 3.4. Wieviele Möglichkeiten gibt es, für eine Schatzsuche eine Klasse mit 21 Schülern in drei Mannschaften zu je sieben Schülern aufzuteilen? Wie hilft die Bahnformel?

Lösung. Sei M die Menge der sämtlichen solchen Aufteilungen (Anordnung der Elemente egal). Wir wollen ihre Ordnung wissen. Wir enumerieren die

Studenten mit den Zahlen $1, \ldots, 21$, und die Gruppe S_{21} wirkt auf M in der offensichtlichen Art. Diese Wirkung ist transitiv. Sei $A \in M$ die Aufteilung

$$A = [1 \text{ bis } 7][8 \text{ bis } 14][15 \text{ bis } 21]$$

Wir haben eine Einbettung $G := (S_7 \times S_7 \times S_7) \times S_3 \hookrightarrow S_{21}$ derart, dass $(\sigma_1, \sigma_2, \sigma_3, \rho) \in G$ auf $\{1, \ldots, 21\}$ wirkt, indem σ_1 auf $\{1, \ldots, 7\}$ wirkt, σ_2 auf $\{8, \ldots, 14\}$, σ_3 auf $\{17, \ldots, 24\}$ und ρ permutiert diese drei Teilmengen (explizit z.B. $(12) \in S_3$ tauscht $1 \leftrightarrow 8$, $2 \leftrightarrow 9$ aus und so weiter). Man sieht, dass G ist genau die Standgruppe von A.
Da $S_{21} \curvearrowright M$ transitiv ist, haben wir $\#(\text{Bahn von } A) = \#M$. Wir setzten die Bahnformel ein und schließen daraus, dass

$$\#M = \frac{\#S_{21}}{\#G} = \frac{21!}{3! \cdot 7!^3} = 66.512.160. \qquad \square$$

Übungen 4 Lösungen: Algebra und Zahlentheorie

Übung 4.1. Man gebe eine Kompositionsreihe der symmetrischen Gruppe S_4 an.
Lösungen. Eine mögliche Reihe:

$$S_4 \to A_4 \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 1 \tag{1}$$

A_4 normal in S_4 da Kern von sgn, in Übung 2.2 hatten wir gezeigt, dass $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ normal in S_4 ist also auch in A_4, die anderen Gruppen sind trivialerweise Normalteiler. Die Quotienten sind alle der Ordnung 3 oder 2 und somit einfach.

Übung 4.2. Man zeige: Jede Untergruppe einer nilpotenten Gruppe ist nilpotent.
Lösungen. G besitzt eine Folge aus Normalteilern, $G = G_r \supset ... \supset G_1 = 1$ mit $G_i/G_{i-1} \subset Z(G/G_{i-1})$. Sei $H \supset G$ nun eine Untergruppe. Betrachte die Folge $H = B_r \supset ... \supset B_1 = 1$ mit $B_i = H \cap G_i$. B_i Normalteiler von H ist klar. Wir zeigen also noch $B_i/B_{i-1} \subset Z(H/B_{i-1})$, betrachte dafür folgende Rechnung.

$$\begin{aligned} B_i/B_{i-1} = (H \cap G_i)/(H \cap G_{i-1}) &\overset{(1)}{=} G_{i-1} \cdot (H \cap G_i)/G_{i-1} \\ &\overset{(2)}{\subset} ((G_{i-1} \cdot H) \cap G_i)/G_{i-1} = (G_{i-1}H/G_{i-1}) \cap (G_i/G_{i-1}) \\ &\subset (G_{i-1}H/G_{i-1}) \cap Z(G/G_{i-1}) \overset{(3)}{\subset} Z(HG_{i-1}/G_{i-1}) \\ &= Z(H/(H \cap G_{i-1})) \overset{(4)}{=} Z(H/B_{i-1}) \end{aligned}$$

(1) und (4) ist ein noetherscher Isomorphiesatz, (2) ist leicht nachzurechnen man muss nur nutzen, dass $G_{i-1} \subset G_i$ gilt und (3) folgt direkt aus

$G_{i-1}H/G_{i-1} \subset G$.
Wir haben also eine passende Kette für H gefunden, H ist Nilpotent.

Übung 4.3. Man zeige: Für jede Primzahl p gibt es bis auf Isomorphismus genau zwei Gruppen der Ordnung $2p$, eine zyklische Gruppe und eine Diedergruppe. Hinweis: Man erinnere die Argumentation im Fall $p = 3$ und interessiere sich für die Anzahl der 2-Sylows.
Lösungen. G besitzt nach den Sylowsätzen entweder eine oder p 2-Sylows.
Fall 1: G besitzt p 2-Sylows. G hat p Elemente der Ordnung 2. Nach Cauchy existiert auch ein Element b der Ordnung p. Sei a ein Element der Ordnung 2 dann gilt $ord(ab) = 2$, die Struktur ist eindeutig als Diedergruppe festgelegt.
Fall 2: G besitzt eine 2-Sylow. G besitzt nach den Sylowsätzen sowieso nur eine p-Sylow. Daraus folgt, dass es mindestens ein Element der Ordnung $2p$ geben muss. Die Gruppe ist also Zyklisch.

Übung 4.4. Wieviele p-Sylows hat die Gruppe $GL(2; \mathbb{F}_p)$?
Lösungen. Bestimme erstmal die Ordnung von $G = GL(2; \mathbb{F}_p)$, zähle dafür die Anzahl der 2-Tupel von linear unabhängigen Vektoren wie in Übung 1.2 um $|G| = (p^2 - 1)(p^2 - p)$ zu erhalten.
Es ist leicht zu sehen, dass $M = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ eine der p-Sylows erzeugt. Betrachte nun die Gruppenwirkung von G auf die Untergruppen von G durch Konjugation. Nach dem zweiten Sylowsatz gilt, dass die Mächtigkeit der Bahn von M gleich der Anzahl von p-Sylows n_p ist. Mit der Bahnenformel erhalten wir also $n_p = |G|/|G_M|$. Wir brauchen also nur noch

$$|G_M| = |\{g \in G \mid g\langle M\rangle g^{-1} = \langle M\rangle\}|$$

zu bestimmen. Rechne also

$$\begin{aligned}
&\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \\
&= \begin{pmatrix} (ad - bc - acm)/(ad - bc) & ma^2/(ad - bc) \\ -mc^2/(ad - bc) & (ad - bc + mac)/(ad - bc) \end{pmatrix} \\
&= \begin{pmatrix} 1 - (mac/ad - bc) & ma^2/ad - bc \\ -mc^2/ad - bc & 1 + (mac/ad - bc) \end{pmatrix}
\end{aligned}$$

Diese Matrix ist genau dann in $\langle M \rangle$ wenn $c = 0$. G_M hat also Ordnung $(p-1)(p^2-p)$, womit wir $n_p = p + 1$ erhalten.

Übungen 5 Lösungen: Algebra und Zahlentheorie

December 18, 2024

Übung 5.1. Gegeben eine endliche Menge X und eine Abbildung $f : X \to X$ zeige man, daß es natürliche Zahlen m, n gibt mit $n \geq 1$ und $f^m = f^{m+n}$.
Lösungen. Sei $|X| = N$. Dann gibt es für jedes der N Elemente von X N-viele Möglichkeiten es abzubilden. Also hat die Menge der Selbstabbildungen von X die Mächtigkeit $|\mathrm{Ens}(X, X)| = N^N$. Alle Verknüpfungen $f^k, k \in \mathbb{N}$, von f sind natürlich auch Abbildungen $X \to X$. Wir setzen $N^N = M$. Angenommen $f, f^2, ..., f^M$ sind alle verschieden. Dann ist

$$\mathrm{Ens}(X, X) = \{f, f^2, ..., f^M\}.$$

Es gibt also $j \in \{1, ..., M\}$ mit $f^{M+1} = f^j$. Dann ist

$$f^{M+(M-j+1)} = f^{M+1} f^{M-j} = f^j f^{M-j} = f^M, \quad \text{und } M - j + 1 \geq 1.$$

Also erfüllen $m = M$ und $n = M - j + 1$ die Behauptung.
Nun angenommen die $f, f^2, ..., f^M$ sind nicht verschieden. Dann gibt es $i, j \in \{1, ..., M\}$ mit $f^i = f^j$. Ohne Einschränkung ist $j > i$, also $j = i + l$ mit $l \geq 1$. Dann erfüllen $m = i$ und $n = l$ die Behauptung.

Übung 5.2. Man zeige, daß das Bild eines Ideals unter einem surjektiven Ringhomomorphismus stets wieder ein Ideal ist.
Lösungen. Sei $\varphi : R \twoheadrightarrow S$ ein surjektiver Ringhomomorphismus und $I \subset R$ ein Ideal. Wir zeigen zunächst, dass $\varphi(I) \subset S$ eine abelsche Untergruppe ist. Erstens ist $0 = \varphi(0) \in \varphi(I)$. Zweitens gibt es für $j, j' \in \varphi(I)$ Elemente $i, i' \in I$ mit $j = \varphi(i)$ und $j' = \varphi(i')$ und somit

$$j + j' = \varphi(i) + \varphi(i') = \varphi(i + i') \in \varphi(I)$$

und

$$0 = \varphi(i + (-i)) = \varphi(i) + \varphi(-i), \quad \text{also } -j = -\varphi(i) = \varphi(-i) \in \varphi(I).$$

Nun zeigen wir die Idealeigenschaft. Seien $j \in \varphi(I)$ und $s \in S$. Dann gibt es $i \in I$ mit $\varphi(i) = j$ und $r \in R$ mit $\varphi(r) = s$, letzteres da φ surjektiv ist. Also gilt

$$j \cdot s = \varphi(i) \cdot \varphi(r) = \varphi(i \cdot r) \in \varphi(I)$$

und

$$s \cdot j = \varphi(r) \cdot \varphi(i) = \varphi(r \cdot i) \in \varphi(I).$$

Somit ist alles gezeigt.

Übung 5.3. Man zeige, daß es für jeden Ring R genau einen Ringhomomorphismus $\mathbb{Z} \to R$ gibt.
Lösungen. Jeder Ringhomomorphismus $\psi : \mathbb{Z} \to R$ muss $\psi(1_\mathbb{Z}) = 1_R$ und $\psi(0_\mathbb{Z}) = 0_R$ erfüllen. Wir behaupten, dass ψ dadurch schon eindeutig festgelegt ist. In der Tat gilt für $n \in \mathbb{N}$:

$$\psi(n) = \psi(\underbrace{1_\mathbb{Z} + ... + 1_\mathbb{Z}}_{n-\text{mal}}) = \underbrace{\psi(1_\mathbb{Z}) + ... + \psi(1_\mathbb{Z})}_{n-\text{mal}} = \underbrace{1_R + ... + 1_R}_{n-\text{mal}}.$$

Seien $-1_\mathbb{Z} \in \mathbb{Z}$ und $-1_R \in R$ die additiven Inversen der jeweiligen Einsen. Dann ist $\psi(-1_\mathbb{Z}) = -1_R$, da $0 = \psi(1_\mathbb{Z} + (-1_\mathbb{Z})) = \psi(1_\mathbb{Z}) + \psi(-1_\mathbb{Z}) = 1_R + \psi(-1_\mathbb{Z})$. Also gilt weiter

$$\psi(-n) = \psi(-1_\mathbb{Z} \cdot n) = \psi(-1_\mathbb{Z}) \cdot \psi(n) = -1_R \cdot (\underbrace{1_R + ... + 1_R}_{n-\text{mal}}) = \underbrace{(-1_R) + ... + (-1_R)}_{n-\text{mal}}.$$

Übung 5.4. Man finde das multiplikative Inverse der Nebenklasse von 22 im Körper $\mathbb{F}_{31}$. Hinweis: Euklidischer Algorithmus.
Lösungen. Nach dem Lemma von Bezout gibt es $a, b \in \mathbb{Z}$ mit

$$a \cdot 22 + b \cdot 31 = \text{ggT}(22, 31) = 1.$$

Wir suchen also $a \pmod{31}$. Mit dem euklidischen Algorithmus erhalten wir

$$\begin{aligned} 31 &= 1 \cdot 22 + 9, \\ 22 &= 2 \cdot 9 + 4, \\ 9 &= 2 \cdot 4 + 1. \end{aligned}$$

Also rückwärts:

$$1 = 5 \cdot 31 - 7 \cdot 22.$$

Also ist $-7 \equiv 24 \pmod{31}$ das multiplikative Inverse von 22 im Körper $\mathbb{F}_{31}$.

Übungen 6 Lösungen: Algebra und Zahlentheorie

18. Dezember 2024

Übung 6.1. Man zeige: Eine natürliche Zahl, die kongruent zu sieben ist modulo acht, kann nicht die Summe von drei Quadraten sein.
Lösung: Betrachtet man die Quadratzahlen in $\mathbb{Z}/8\mathbb{Z}$, so stellt man fest, dass die einzigen Quadratzahlen $0, 1$ und 4 sind:

$$0^2 = 0 \qquad 1^2 = 1 \qquad 2^2 = 4 \qquad 3^2 = 9 \equiv 1$$
$$4^2 = 16 \equiv 0 \qquad 5^2 = 25 \equiv 1 \qquad 6^2 = 36 \equiv 4 \qquad 7^2 = 49 \equiv 1$$

Damit kann man einfach alle möglichen Summen von 3 Quadratzahlen in $\mathbb{Z}/8\mathbb{Z}$ berechnen. Man beachte dass Summen, die zwei mal die 4 enthalten ignoriert werden können, da $4 + 4 = 0 + 0 \pmod 8$. Es ergeben sich die Möglichkeiten:

$$0+0+0=0 \qquad 0+1+1=2$$
$$0+0+1=1 \qquad 0+1+4=5$$
$$0+0+4=4 \qquad 1+1+1=3$$
$$1+1+4=6$$

Insbesondere kann die Summe von drei Quadratzahlen in $\mathbb{Z}/8\mathbb{Z}$ nie $= 7$ sein, was zu zeigen war. □

Übung 6.2. Man finde ein Nichtquadrat a im Körper $\mathbb{F}_5$ und zeige, dass der Restklassenring $\mathbb{F}_5[X]/\langle X^2 - a\rangle$ ein Körper mit 25 Elementen ist.
Lösung: Diese Aussage folgt schnell durch die Anwendung einiger Sätze der Vorlesung: Da a Nichtquadrat ist, ist $X^2 - a$ irreduzibel in $\mathbb{F}_5[X]$ und erzeugt damit ein maximales Ideal. Damit ist der Quotient $\mathbb{F}_5[X]/\langle X^2 - a\rangle$ ein

Körper.
Ich vermute aber, dass die Idee der Aufgabe war, das für dieses Beispiel einmal konkret nachzurechnen. Dies werde ich deshalb im Folgenden tun:
Die Quadrate in $\mathbb{F}_5$ sind $0^2 = 0, 1^2 = 1, 2^2 = 4, 3^2 \equiv 4$ und $4^2 \equiv 1$. Damit sind 2 und 3 mögliche Nichtquadrate, die man für a wählen könnte.
Gegeben ein Polynom in $\mathbb{F}_5[X]$ von Grad ≥ 2 kann man den Grad durch Abziehen eines passenden Vielfachen von $X^2 - a$ verringern. Also hat jedes Element in $\mathbb{F}_5[X]/\langle X^2 - a\rangle$ einen Repräsentanten der Form $bX + c$ mit $b, c \in \mathbb{F}_5$. Da diese paarweise nicht äquivalent sein können (ihre Differenz hat höchstens Grad 1) sieht man auch, das $\mathbb{F}_5/\langle X^2 - a\rangle$ 25 Elemente haben muss.
Ich behaupte nun, das Inverse von $[bX + c]$ ist $\left[\frac{1}{ab^2+c^2}(-bX + c)\right]$ (Dieses Inverse findet man z.B. durch eine Rechnung analog zur Rationalisierung des Nenners.) Die Behauptung überprüft man durch Nachrechnen:
Für ein Element $[bX + c] \in (\mathbb{F}_5/\langle X^2 - a\rangle) \setminus \{[0]\}$ gilt:

$$\begin{aligned}(bX + c) \cdot \frac{1}{ab^2 + c^2}(-bX + c) &= (-b^2X^2 + c^2)\frac{1}{ab^2 + c^2} \\ &\equiv (-b^2X^2 + b^2 \cdot (X^2 - a) + c^2)\frac{1}{ab^2 + c^2} \\ &= (ab^2 + c^2)\frac{1}{ab^2 + c^2} \\ &= 1\end{aligned}$$

Es muss noch überprüft werden, dass $\frac{1}{ab^2+c^2}$ tatsächlich existiert, also das ab^2+c^2 in $\mathbb{F}_5$ invertierbar, also nicht Null ist. Wir wissen dass a kein Quadrat ist und dass $bX + c$ ungleich Null sein muss. Wäre $ab^2 + c^2 = 0$ so würde folgen:

$$ab^2 = -c^2 \Rightarrow \begin{cases} a = \frac{-c^2}{b^2} = \left(\frac{-c}{b}\right)^2 & \text{falls } b \neq 0 \\ c^2 = 0 \Rightarrow c = 0 & \text{falls } b = 0 \end{cases}$$

Das ist ein Widerspruch zu a ist kein Quadrat bzw. $bX + c \neq 0$. Damit existiert das angegebene Inverse und $\mathbb{F}_5[X]/\langle X^2 - a\rangle$ ist ein Körper. □

Übung 6.3. Man zeige, dass $\mathbb{Z}[X]$ kein Hauptidealring ist.
Lösung: Betrachte das Ideal $\langle X, 2\rangle \subseteq \mathbb{Z}[X]$. Ich behaupte, dass dies kein Hauptideal ist. Angenommen $\langle X, 2\rangle \subseteq \mathbb{Z}[X]$ wäre ein Hauptideal, also erzeugt von einem Element $a \in \mathbb{Z}[X]$. Dann müsste a ein Teiler von X und

von 2 sein. Die einzigen Teiler von $X \in \mathbb{Z}[X]$ sind ± 1 und $\pm X$ und die einzigen Teiler von $2 \in \mathbb{Z}[X]$ sind ± 1 und ± 2. Damit wäre aber $a = \pm 1$, also $\langle \pm 1 \rangle = \langle X, 2 \rangle$. Jedoch gilt $1 \notin \langle X, 2 \rangle = \{\sum a_i X^i \mid a_i \in \mathbb{Z}, a_0 \in 2\mathbb{Z}\}$, Widerspruch!
Also kann $\langle X, 2 \rangle \subseteq \mathbb{Z}[X]$ kein Hauptideal und damit $\mathbb{Z}[X]$ kein Hauptidealring sein.

Übung 6.4. Sei k ein Körper. Man zeige:
(1) Alle Polynome vom Grad 1 sind irreduzibel in $k[X]$.
(2) Ist $P \in k[X]$ irreduzibel und $\operatorname{grad} P > 1$*, so hat P keine Nullstelle in k.*
(3) Ist $P \in k[X] \setminus k$ vom Grad $\operatorname{grad} P \leq 3$ *und hat P keine Nullstelle in k, so ist P irreduzibel in $k[X]$.*
(4) Ist k algebraisch abgeschlossen, so sind die irreduziblen Polynome in $k[X]$ genau die Polynome vom Grad 1.
Man gebe (5) ein Polynom positiven Grades in $\mathbb{R}[X]$ an, das keine Nullstelle hat, aber dennoch nicht irreduzibel ist.
Lösung: Sei im folgenden immer P das in der Aufgabenstellung beschriebene Polynom, und $Q, R \in k[X]$ Polynome mit $Q \cdot R = P$. Man beachte außerdem, dass die Einheiten in $k[X]$ genau die Elemente von $k \setminus \{0\}$ sind.

(1) Da $\operatorname{grad} P = 1$ müssen Q oder R von Grad 0 sein, da $\operatorname{grad} Q + \operatorname{grad} R = \operatorname{grad} P$. Also ist Q oder R insbesondere in k und damit Einheit in $k[X]$. Also ist P irreduzibel.

(2) Angenommen P hätte eine Nullstelle a in k. Wir können durch Polynomdivision P schreiben als $P = (X - a) \cdot S + T$ mit $S, T \in k[X]$ und $\operatorname{grad} T < \operatorname{grad}(X - a) = 1$, also $T \in k$. Da a Nullstelle ist, folgt durch Einsetzen von a dass sogar $T = 0$ ist und damit $P = (X - a) \cdot S$. Weil $\operatorname{grad} S = \operatorname{grad} P - \operatorname{grad}(X - a) = \operatorname{grad} P - 1 > 1 - 1 = 0$ ist, ist S keine Einheit und damit P reduzibel. Also können irreduzible Polynome von Grad > 1 keine Nullstelle haben.

(3) Da $\operatorname{grad} P \leq 3$ muss einer der Faktoren Q oder R von Grad ≤ 1 sein. (Sonst wäre $gradP \geq 4$.) Sei o.B.d.A Q dieser Faktor. Wäre $\operatorname{grad} Q = 1$, wäre $Q = aX + b$ mit $a, b \in k$. Damit wäre aber $Q(\frac{-b}{a}) = 0$, also $\frac{-b}{a} \in k$ eine Nullstelle von Q und damit auch von P. Also muss $\operatorname{grad} Q = 0$ sein und damit Q eine Einheit. Also war P irreduzibel.

(4) Nach (1) sind alle Polynome von Grad 1 irreduzibel. In algebraisch abgeschlossenen Körpern haben nichtkonstante Polynome immer eine Nullstelle, also sind nach (2) Polynome von Grad $\operatorname{grad} P > 1$ nicht irreduzibel. Polynome von Grad 0 sind Einheiten. Also sind die irreduziblen Polynome

in $k[X]$ für algebraisch abgeschlossenes k genau die Polynome von Grad 1.

(5) $P = X^4 + 3X^2 + 2 = (X^2 + 1)(X^2 + 2)$ hat keine Nullstellen in $\mathbb{R}$, da $a^2 \geq 0$ für alle $a \in \mathbb{R}$, aber ist offensichtlich reduzibel.

Übungen Lösungen: Algebra und Zahlentheorie

December 19, 2024

Übung 7.1. Man schreibe $9 + 13i$ als Produkt von Gaußprimzahlen
Lösungen. We use the algorithm in Mathstackexchange/1562858, which works as 9 and 13 are coprime. The norm of $9 + 13i$ is 250. We factor $250 = 2 * 5^3 = i(1 - i)^2 * (2 + i)^3(2 - i)^3$. For each conjugate pair except the ones which divide 2, we discard one of the pair, to see which one: divide $9 + 13i$ by it to see if we are left with a Gaussian integer. Observe that $(9+13i)/(2-i) = (5+35i)/5 = 1+7i$. So $9+13i = (i-1)(2-i)^3$, adjusting by a unit.

Übung 7.2. Man bestimme sämtliche Zerlegungen von 1000 *in eine Summe von zwei Quadratzahlen.*
Lösungen. Write $1000 = 2^3 * 5^3$. The sum of squares function tells us that there are precisely two decompositions of 1000 as a sum of two squares. These are $1000 = 10^2 + 30^2 = 18^2 + 26^2$. Can do this by trial and error, or alternatively, use the algorithm described in Mathstackexchange 2536097.

Übung 7.3. Seien R ein faktorieller Ring und $q \in Quot(R)$ ein Element seines Quotientenkörpers und $n \geq 1$ mit $q^n \in R$. Man zeige $q \in R$.
Lösungen. By assumption $q^n - r = 0$, for some $r \in R$. Write $q = a/b$, for $a, b \in R$, where a, b have no non-unit common divisor (this is possible as R is a UFD). Multiplying by b^n gives us $a^n - rb^n = 0$. Let d be an irreducible divisor of b. Then d is prime as R is a UFD. Since d divides $rb^n = a^n$, it must divide a (as it is prime). Since a, b have no non-unit common divisors, d is a unit. So b is also a unit, and $u \in R$. More generally, this follows from the fact that every UFD is integrally closed.

Übung 7.4. Man bestimme die Partialbruchzerlegung von $1/(x^4+2)$ *in* $\mathbb{C}(X)$.
Lösungen. Let z denote the real positive 4'th root of $1/2$. The roots of x^4+2 over $\mathbb{C}$ are $z(\pm 1 \pm i)$. Writing as partial fractions gives us

$$\frac{1}{x^4+2} = \frac{a}{x-z(1+i)} + \frac{b}{x+z(1+i)} + \frac{c}{x-z(1-i)} + \frac{d}{x+z(1-i)},$$

where $-a = b = z^{13}(1+i)$ and $-c = d = z^{13}(1-i)$.

Übungen 8 Lösungen: Algebra und Zahlentheorie

December 20, 2024

Übung 8.1. Seien k ein Körper und $0 < n(1) < n(2) < \ldots < n(r) < n$ natürliche Zahlen, $r \geq 0$. Man zeige, dass das Polynom

$$T^n + a_r T^{n(r)} + \ldots + a_1 T^{n(1)} + a_0$$

irreduzibel ist in $K[T]$, für $K = \operatorname{Quot} k[`a_0, \ldots, a_r]$ der Funktionenkörper. Hinweis: Jede Zerlegung käme von einer Zerlegung im Polynomring $k[`a_0, \ldots, a_r, T]$ her und müsste unter dem Einsetzen $a_1 = ... = a_r = 0$ zu einer Zerlegung von $T^n + a_0$ in $k[`a_0, T]$ führen.

Lösungen. Wir folgen dem Vorgehen aus dem Hinweis: Angenommen das Polynom P hätte eine Zerlegung in $K[T]$, dann fänden wir auch eine Zerlegung $P = AB$ mit $A, B \in k[`a_0, \ldots, a_r, T]$. Setzen wir nun $a_1 = ... = a_r = 0$ ein, so erhalten wir eine Zerlegung von $T^n + a_0$. Dieses Polynom ist aber nach dem (allgemeinen) Eisensteinkriterium irreduzibel. Also muss einer der Faktoren eine Einheit in $k[`a_0, T]$ sein und damit ist ohne Einschränkung A ein Polynom in $k[`a_1, \ldots, a_r]$. Das ist ein Widerspruch zu $P = AB$.

Übung 8.2. Man zeige, dass $X^7 - 9$ ein irreduzibles Polynom in $Z[X]$ ist. Hinweis: Man betrachte die Einbettung $\mathbb{Z}[X] \hookrightarrow \mathbb{Z}[Y]$ mit $X \mapsto Y^2$.

Lösungen. Die Einbettung ι aus dem Hinweis bildet unser Polynom P wie folgt ab: $X^7 - 9 \mapsto Y^{14} - 9 = (Y^7 - 3)(Y^7 + 3)$. Die beiden Faktoren sind mit Eisenstein irreduzibel in $\mathbb{Z}[Y]$. Gälte $P = AB$ mit A, B irreduzibel in $\mathbb{Z}[X]$, erhielten wir $\iota(A) \big| \iota(P)$. Jedoch ist $\iota(A) \neq (Y^7 \pm 3)$, da Polynome mit Termen ungeraden Grades nicht im Bild von ι liegen. Also ist A oder B eine Einheit und P irreduzibel.

Übung 8.3. Man zerlege $(X^n - Y^n)$ in $\mathbb{C}[X,Y]$ in ein Produkt irreduzibler Faktoren.

Lösungen. $\mathbb{C}[X,Y]$ ist faktoriell, daher existiert eine solche eindeutige Zerlegung. Wir schreiben $X^n - Y^n = Y^n((X/Y)^n - 1)$ aufgefasst in $\mathbb{C}(X,Y)$. Mit $Z^n - 1 = \prod_{\zeta^n=1}(Z-\zeta)$ in $\mathbb{C}[Z]$ erhalten wir

$$\begin{aligned} X^n - Y^n &= Y^n\left(\left(\frac{X}{Y}\right)^n - 1\right) \\ &= Y^n \prod_{\zeta^n=1}\left(\frac{X}{Y} - \zeta\right) \\ &= \prod_{\zeta^n=1}(X - \zeta Y). \end{aligned}$$

Wobei die letzte Gleichheit gilt, da es n verschiedene n-te Einheitswurzeln gibt und das Produkt daher n Faktoren hat. Jedes der Polynome ist als Polynom von Grad 1 irreduzibel, also haben wir die gesuchte Darstellung gefunden.

Übung 8.4. Was ist die Summe der $\lambda_1^3 + \lambda_2^3 + \lambda_3^3 + \lambda_4^3$ dritten Potenzen der vier komplexen Nullstellen $\lambda_1, \ldots, \lambda_4$ des Polynoms $X^4+3X^3-5X^2+X+1$?

Lösungen. Es gilt nach Aufgabenstellung $X^4 + 3X^3 - 5X^2 + X + 1 = (X - \lambda_1)(X - \lambda_2)(X - \lambda_3)(X - \lambda_4)$. Mit dem Satz von Vieta bzw. Koeffizientenvergleich erhalten wir

$$\begin{aligned} 1 &= s_4 = \lambda_1\lambda_2\lambda_3\lambda_4 \\ -1 &= s_3 = \lambda_1\lambda_2\lambda_3 + \lambda_1\lambda_2\lambda_4 + \lambda_1\lambda_3\lambda_4 + \lambda_2\lambda_3\lambda_4 \\ -5 &= s_2 = \lambda_1\lambda_2 + \lambda_1\lambda_3 + \lambda_1\lambda_4 + \lambda_2\lambda_3 + \lambda_2\lambda_4 + \lambda_3\lambda_4 \\ -3 &= s_1 = \lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 \end{aligned}$$

wobei die s_i die elementarsymmetrischen Polynome bezeichnen. Multiplizieren wir nun den Ausdruck $(\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4)^3$ aus und stellen um, erhalten wir

$$\begin{aligned} &\lambda_1^3 + \lambda_2^3 + \lambda_3^3 + \lambda_4^3 \\ =&(\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4)^3 - 6(\lambda_1\lambda_2\lambda_3 + \lambda_1\lambda_2\lambda_4 + \lambda_1\lambda_3\lambda_4 + \lambda_2\lambda_3\lambda_4) \\ &- 3(\lambda_1(\lambda_1\lambda_2 + \lambda_1\lambda_3 + \lambda_1\lambda_4) + \lambda_2(\lambda_2\lambda_1 + \lambda_2\lambda_3 + \lambda_2\lambda_4) \\ &+ \lambda_3(\lambda_3\lambda_1 + \lambda_3\lambda_2 + \lambda_3\lambda_4) + \lambda_4(\lambda_4\lambda_1 + \lambda_4\lambda_2 + \lambda_4\lambda_3)) \\ =&s_1^3 - 6s_3 - 3(s_1s_2 - 3s_3) \end{aligned}$$

wobei man die letzte Gleichheit leicht nachrechnet. Einsetzen liefert

$$\lambda_1^3 + \lambda_2^3 + \lambda_3^3 + \lambda_4^3 = (-3)^3 + 6 - 3(15 + 3) = -27 + 6 - 54 = -75.$$

Übungsblatt 9 Lösungen: Algebra und Zahlentheorie

Übung 9.1. Gegeben $a, b \in \mathbb{Q}^\times$ zeige man, daß gilt $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{b})$ genau dann, wenn $\frac{a}{b}$ in $\mathbb{Q}$ ein Quadrat ist. Zum Beispiel folgt $\sqrt{5} \notin \mathbb{Q}(\sqrt{2})$.
Lösung. Wenn a oder b ein Quadrat in $\mathbb{Q}$ ist, ist die Aussage offensichtlich. Ebenfalls die Richtung $\frac{a}{b} \in (\mathbb{Q}^\times)^2 \implies \mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{b})$. Nehmen wir an, dass $a, b \notin (\mathbb{Q}^\times)^2$. Dann

$$\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{b}) \implies \sqrt{a} = \alpha + \beta\sqrt{b}$$

für irgendwelche $\alpha, \beta \in \mathbb{Q}$. ($\beta$ muss nicht null sein, also mit Umschreiben der Gleichung gilt " $\Longleftarrow$ " auch). Wir nehmen das Quadrat von beiden Seiten und es wird klar, dass $\alpha = 0$ denn $\sqrt{b}$ ist nicht rational. Deswegen gilt

$$\sqrt{\frac{a}{b}} = \beta \in \mathbb{Q}^\times,$$

und deshalb $\frac{a}{b} \in (\mathbb{Q}^\times)^2$. $\square$

Übung 9.2. Seien K ein Körper und $P \in K[X] \setminus K$ ein nichtkonstantes Polynom. So ist der Ringhomomorphismus $K[Y] \mapsto K[X]$ mit $Y \mapsto P$ injektiv und die davon induzierte Körpererweiterung $K(Y) \mapsto K(X)$ hat als Grad den Grad von P.
Lösung. Wir bezeichnen mit $K(P)$ das Bild von $K(Y)$ in $K(X)$, nämlich rationale Funktionen im Polynom P. Dann als Körpererweiterung von $K(P)$ wird $K(X)$ von X erzeugt. Dann bleibt es nur, den Grad vom Minimalpolynom von X über $K(P)$ zu bestimmen. Wir haben natürlich

$$P(T) - P \in K(P)[T] \text{ verschwindet, wenn } T = X$$

also ist $K(X)/K(P)$ inbesondere eine endliche Erweiterung, und $1, X, \ldots, X^{d-1}$ erzeugen $K(X)$ als $K(P)$-Vektorraum, $d = \deg P$. Nehmen wir an, dass diese Elemente linear abhängig sind, und zwar sie erfüllen eine nicht triviale lineare Gleichung. Nachdem wir die Nenner durch Multiplikation entfernen, erhalten wir eine Gleichung in $K[X]$ der Form

$$f_{d-1}(P)X^{d-1} + f_{d-2}(P)X^{d-2} + \cdots + f_0(P) = 0, \quad f_i \in K[T].$$

Wir nehmen ein f_i mit $\deg f_i = \max_j \deg f_j$. Dann ist der Koeffizient von $X^{i+d\deg f_i}$ nicht null auf der linken Seite, was einen Widerspruch ergibt. Deswegen muss jedes $f_j = 0$. □

Übung 9.3. Alle Elemente von $\mathbb{Q}(\sqrt[3]{2})$ lassen sich eindeutig schreiben in der Form $a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2$ mit $a, b, c \in \mathbb{Q}$. Man schreibe das Inverse von $7 + \sqrt[3]{2}$ in dieser Form.
Lösung.

$$\frac{\mathbb{Q}[T]}{(T^3 - 2)} \xrightarrow{\sim} \mathbb{Q}(\sqrt[3]{2}), \quad T \mapsto \sqrt[3]{2},$$

da $T^3 - 2$ irreduzibel ist. Die linke Seite wird natürlich von $1, T, T^2$ als $\mathbb{Q}$-Vektorraum erzeugt, deswegen lässt sich jedes Element auf der rechten Seite als $\mathbb{Q}$-lineare Summe von $1, \sqrt[3]{2}, (\sqrt[3]{2})^2$ schreiben.

Nun bestimmen wir das Inverse von $7 + \sqrt[3]{2}$. Wir wollen $a, b, c \in \mathbb{Q}$ so, dass

$$(7 + \sqrt[3]{2})(a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2) = (7a + c) + \sqrt[3]{2}(a + 7b) + (\sqrt[3]{2})^2(7c + b) = 1.$$

Wir finden die eindeutige Lösung $a = \frac{49}{345}, b = -\frac{7}{345}, c = \frac{1}{345}$. □

Übung 9.4. Ist $\sqrt{2} + \sqrt{3}$ algebraisch über $\mathbb{Q}$? Wenn ja, was ist sein Minimalpolynom über $\mathbb{Q}$? Liegt $\sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$?.
Lösung. Wir setzen $x = \sqrt{2} + \sqrt{3}$. Einfache Rechnung liefert

$$\begin{aligned} x^2 &= 5 + 2\sqrt{6} \\ x^3 &= 9x + 2\sqrt{2} \\ x^4 &= 9x^2 + 4 + 2\sqrt{6}. \end{aligned}$$

Wir können schon aus der zweiten Gleichung schließen, dass $\sqrt{2} \in \mathbb{Q}(x)$. Wir bemerken von der ersten und dritten auch, dass $x^4 - 10x^2 + 1 = 0$, also ist

x algebraisch. Wir müssen nur beweisen, dass dieses Polynom irreduzibel ist. Nach dem Gauß'schen Lemma ist es irreduzibel genau dann, wenn es irreduzibel über $\mathbb{Z}$ ist. Falls $x^4 - 10x^2 + 1 = (x^2 + ax + b)(x^2 + cx + d)$ mit $a, b, c, d \in \mathbb{Z}$,

$$\begin{aligned} bd &= 1 \\ a + c &= 0 \\ b + ac + d &= -10 \\ bc + ad &= 0. \end{aligned}$$

Also $-ac$ ist ein Quadrat aber zusätzlich $-ac = 10 + b + d = 10 \pm 2$, was ein Widerspruch ist. Falls $x^4 - 10x^2 + 1 = (x^3 + ax^2 + bx + c)(x - d)$,

$$\begin{aligned} a &= d \\ c &= bd \\ -cd &= 1 \\ b - ad &= -10. \end{aligned}$$

Dann haben c, d Betrag 1 und deshalb auch a und b. Aber es folgt, dass $|b - ad| \leq 2$, was einen Widerspruch zur letzten Gleichung ergibt. $\square$

Übungen 10 Lösungen: Algebra und Zahlentheorie

Übung 10.1. Geben Sie einen Körperisomorphismus $\mathbb{F}_7(\sqrt{3})\tilde{\to}\mathbb{F}_7(\sqrt{5})$ *an als* $\mathbb{F}_7$*-Lineare Abbildung in Bezug auf die Basen* $1, \sqrt{3}$ *links und* $1, \sqrt{5}$ *rechts.*
Lösungen. Eine lineare Abbildung ist eindeutig definiert über die Werte, die die Basiselemente annehmen. Definiere $\phi : \mathbb{F}_7(\sqrt{3}) \to \mathbb{F}_7(\sqrt{5})$ also durch $\phi(1) = 1$ und $\phi(\sqrt{3}) = 3\sqrt{5}$. Es gilt $\phi(\sqrt{3}\sqrt{3}) = \phi(3) = 3 = 3\sqrt{5}3\sqrt{5} = \phi(\sqrt{3})\phi(\sqrt{3})$. Die dritte Gleichheit folgt da $3 = 45$ in $\mathbb{F}_7(\sqrt{3})$, also ist ϕ ein Körperhomomorphismus.
Die darstellende Matrix von ϕ bezüglich der Basen ist:

$$M = \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}$$

Woran man erkennt, dass es sich um einen Isomorphismus handelt.

Übung 10.2. Man zeige, daß es gegeben eine Primzahl $p > 2$ *und* $r \geq 1$ *stets einen endlichen Körper der Charakteristik* p *gibt, dessen multiplikative Gruppe ein Element der Ordnung* 2^r *hat.*
Lösungen. Sei $p > 2$ Primzahl. Wie im Skript können wir Körpererweiterungen $L \subset \mathbb{F}_p$ mit $|L| = p^m$ für $m \in \mathbb{N}$ konstruieren.
Außerdem sind die multiplikativen Gruppen der L zyklisch und es gilt $|L^*| = p^m - 1$. Wir untersuchen nun die Primfaktorzerlegung von $p^m - 1$ nach Zweierpotenzen. Da p^m ungerade folgt $p^m - 1$ gerade, wir haben also mindestens eine 2 in der Primfaktorzerlegung. Des weiteren haben wir $p^{2m} - 1 = (p^m + 1)(p^m - 1)$ in $p^{2m} - 1$ ist also mindestens eine weitere 2 in der Primfaktorzerlegung enthalten.
Induktiv können wir daraus schließen, dass wir für jedes $n \in \mathbb{N}$ ein m finden können mit $2^n | p^m - 1$.

Sein nun $r \geq 1$, wähle wie oben beschrieben eine endliche Körpererweiterung L der Mächtigkeit p^m von $\mathbb{F}_p$, so dass die höchste $2er$-Potenz n von $p^m - 1$ größer als r ist. Nun haben wir nach den Sylowsätzen eine Untergruppe $U_2 \subset L^*$ mit $|U_2| = 2^n$. Da L^* zyklisch ist auch U_2 zyklisch, es gibt also ein Element $g \in U_2$ mit $g^{2^n} = 1$, dann hat aber $g' = g^{2^{n-r}}$ Ordnung 2^r, da $g'^{2^r} = (g^{2^{n-r}})^{2^r} = g^{2^{n-r}2^r} = g^{2^n} = 1$

Übung 10.3. Gegeben eine endliche Körpererweiterung $K \subset L$ zeige man, daß jedes Polynom aus dem Polynomring $L[X]$ Teiler eines Polynoms aus dem Polynomring $K[X]$ ist.
Lösungen. Wir zeigen die Aussage erst mal für irreduzible Polynome. Sei also P in $L[X]$ ein irreduzibles Polynom und sei es o.B.d.A. normiert (wir können einfach mit einem konstanten Polynom multiplizieren was für Teilbarkeit keine Rolle spielt). Sei $L' \subset L$ eine endliche Körpererweiterung in der P eine Nullstelle α hat. Da P normiert und irreduzibel in L, ist es Minimalpolynom von α für L'/L. Da L/K endlich ist, ist wegen der Gradformel auch L'/K endlich, α hat also ein Minimalpolynom P' über K. Also gilt $P|P'$ in $L[X]$, mit $P' \in K[X]$.
Sei nun $Q \in L[X]$, $L[X]$ ist faktoriell da L Körper, also gilt $Q = P_1, \cdots, P_n$ für P_i irreduzibel. Für jedes P_i finden wir nach dem obigen ein $P_i' \in K$, welches von P_i geteilt wird. Mit der Beobachtung das $a|b$ und $a'|b' \Rightarrow aa'|bb'$ wird die Aussage beweisen.

Übung 10.4. Man zeige: Gegeben eine Primzahl p und zwei p-te Einheitswurzeln $\zeta, \xi \in \mathbb{C}$ der Ordnung p gilt $\mathbb{Q}(\zeta) = \mathbb{Q}(\xi)$ und es gibt genau einen Körperhomomorphismus $\mathbb{Q}(\zeta) \to \mathbb{Q}(\xi)$ mit $\zeta \mapsto \xi$. Hinweis: Irreduzibilität des p-ten Kreisteilungspolynom.
Lösungen. Die erste Aussage folgt direkt daraus, dass ζ und ξ dasselbe Kreisteilungspolynom als Minimalpolynom über $\mathbb{Q}$ haben.
Da $\mathbb{Q}(\zeta)$ eine einfache Körpererweiterung lässt sich ein Element $x \in \mathbb{Q}(\zeta)$ schreiben als $x = \beta_0\zeta^0 + \cdots + \beta_{p-1}\zeta^{p-1}$ mit $\beta_i \in \mathbb{Q}$. Sein nun ϕ ein Körperhomomorphismus wie in der Aufgabe beschrieben, dann gilt

$$\begin{aligned}\phi(x) &= \phi(\beta_0\zeta^0 + \cdots + \beta_{p-1}\zeta^{p-1}) \\ &= \phi(\beta_0)\phi(\zeta)^0 + \cdots + \phi(\beta_{p-1})\phi(\zeta)^{p-1} \\ &= \beta_0\phi(\zeta)^0 + \cdots + \beta_{p-1}\phi(\zeta)^{p-1} \\ &= \beta_0\xi^0 + \cdots + \beta_{p-1}\xi^{p-1}\end{aligned}$$

In der dritten Gleichheit haben wir genutzt, dass Körperhomomorphismen von $\mathbb{Q} \to \mathbb{Q}$ immer die Identität seien müssen. Nun haben wir aber gezeigt, dass ϕ durch die gegebene Abbildungsvorschrift schon eindeutig festgelegt ist.

Übungen 11 Lösungen: Algebra und Zahlentheorie

January 19, 2025

Übung 11.1. Man zeige: Ein Polynom mit Koeffizienten in einem Körper K der Charakteristik Null ist separabel genau dann, wenn es von keinem Quadrat eines K-irreduziblen Polynoms geteilt wird.
Lösungen. Zunächst bemerken wir, dass nach 3.9.17 jedes irreduzible Polynom über char $K = 0$ separabel ist.
Sei nun $P \in K[X]$ separabel. Angenommen es gäbe ein irreduzibles $Q \in K[X]$ mit $Q^2|P$, dann hätte P aber doppelte Nullstellen in seinem Zerfällungskörper, was der Definition von P separabel widerspricht. Andererseits ist nach der Vorbemerkung jedes irreduzible Polynom separabel. Wenn kein Quadrat eines K-irreduzibles Polynoms P teilt, hat P also keine mehrfachen Nullstellen im Zerfällungskörper. Also ist P nach Definition separabel.

Übung 11.2. Finden Sie alle komplexen mehrfachen Nullstellen des Polynoms $P = X^4 - 4X^3 + 5X^2 - 4X + 4$.
Lösungen. Eine mehrfache Nullstelle von P wäre auch eine Nullstelle der Abteilung $P' = 4X^3 - 12X^2 + 10X - 4$. Wir berechnen den größten gemeinsamen Teiler mittels Polynomdivision mit Rest:

$$P : P' = 1/4X - 1/4, \text{ Rest: } r_1 = -1/2X^2 - 1/2X + 3,$$

also $P = P' \cdot (1/4X - 1/4) + r_1$. Jetzt teilen wir P' durch r_1 mit Rest:

$$(4X^3 - 12X^2 + 10X - 4) : (-1/2X^2 - 1/2X + 3) = -8X + 32, \text{ Rest: } r_2 = 50X - 100,$$

also $P' = r_1 \cdot (-8X + 32) + r_2$. Schließlich teilen wir r_1 durch r_2 ohne Rest. Also ist $X - 2$ (habe r_2 mit der Einheit $1/50$ multipliziert) der größte gemeinsame Teiler.

Insbesondere teilt $(X-2)^2$ das Polynom P. Wir machen nochmal Polynomdivision:

$$P : (X-2)^2 = X^2 + 1.$$

Also ist $P = (X-2)^2(X-i)(X+i)$ und 2 ist die einzige mehrfache Nullstelle.

Übung 11.3. Man zeige: Seien $M \supset L \supset K$ Körper. Ist M/L separabel und L/K separabel, so ist M/K separabel. Hinweis: Man ziehe sich zunächst auf den Fall endlicher Erweiterungen zurück und verwende dann den Satz über die Charakterisierungen separabler Körpererweiterungen.

Lösungen.

Wir betrachten zunächst den Fall dass M/K endlich ist. Sei $N \supset M$ die normale Hülle von M/K. Dann reicht es nach Satz 3.9.28 zu zeigen, dass gilt

$$|\mathrm{Hom}_K(M,N)| = [M:K].$$

N/M ist nach Satz 3.8.24 endlich und nach Übung 3.8.27 gilt außerdem, dass N/L normal ist. Nun wissen wir nach Voraussetzung, dass

$$|\mathrm{Hom}_K(L,N)| = [L:K] \quad \text{und} \quad |\mathrm{Hom}_L(M,N)| = [M:L].$$

Durch Einschränkung von K-Homomorphismen erhalten wir eine Abbildung

$$F : \mathrm{Hom}_K(M,N) \to \mathrm{Hom}_K(L,N), \quad \sigma \mapsto \sigma_{|L}.$$

Wir untersuchen die Fasern dieser Abbildung. Für $\tau \in \mathrm{Hom}_K(L,N)$ lässt sich τ nach dem Ausdehnbarkeitskriterium 3.8.12 zu einem K-Homomorphismus $M \to N$ fortsetzen, also ist die Faser $F^{-1}(\tau)$ nicht-leer. Ist $\sigma_0 \in F^{-1}(\tau)$ ein fixiertes Element, das wir fortsetzen zu $\tilde{\sigma_0} : N \to N$ (wieder mit 3.8.12), was dann ein Automorphismus ist. Dann ist die Abbildung

$$F^{-1}(\tau) \to \mathrm{Hom}_L(M,N), \quad \sigma \mapsto \tilde{\sigma_0}^{-1} \circ \sigma$$

eine Bijektion. In der Tat, $\tilde{\sigma_0}^{-1} \circ \sigma$ ist ein L-Homomorphismus, denn für $\alpha \in L$ gilt

$$\tilde{\sigma_0}^{-1} \circ \sigma(\alpha) = \tilde{\sigma_0}^{-1}(\tau(\alpha)) = \tilde{\sigma_0}^{-1}(\sigma_0(\alpha)) = \alpha.$$

Die Bijektivität folgt, da die Umkehrabbildung gegeben ist durch $\sigma \mapsto \tilde{\sigma_0} \circ \sigma$. Jede Faser von $F^{-1}(\tau)$ hat also $|\mathrm{Hom}_L(M,N)|$ viele Elemente. Weil $\mathrm{Hom}_K(M,N)$ die disjunkte Vereinigung der Fasern von F ist und es $|\mathrm{Hom}_K(L,N)|$ viele Fasern gibt, erhalten wir die folgende Gleichheit:

$$|\mathrm{Hom}_K(M,N)| = |\mathrm{Hom}_L(M,N)||\mathrm{Hom}_K(L,N)| = [M:L][L:K] = [M:K].$$

Jetzt betrachten wir den allgemeinen Fall. Sei also $\alpha \in M$ und $\mathrm{Irr}(\alpha, L) = \sum_{i=0}^{n} a_i X^i$. Betrachte die endliche Erweiterung $L' = K(a_0, ..., a_n) \supset K$. Weil α über L separabel ist, hat $\mathrm{Irr}(\alpha, L)$ nur einfache Nullstellen. Deshalb ist α auch separabel über L', denn das Minimalpolynom über L' ist dasselbe Polynom. Weil L über K separabel ist, ist auch L' separabel über K (da jedes Element von L' auch ein Element von L ist). Da die Erweiterungen $L'(\alpha)/L'$ und L'/K endlich und separabel sind, ist auch $L'(\alpha)/K$ separabel nach vorherigem Fall, insbesondere ist α separabel über K.

Übung 11.4. Eine algebraische Körpererweiterung derart, daß nur die Elemente des kleinen Körpers über diesem separabel sind, heißt rein inseparabel. Man zeige, daß eine algebraische Erweiterung L/K eines Körpers K der Charakteristik $p > 0$ rein inseparabel ist genau dann, wenn für jedes Element von L die p^r-te Potenz für hinreichend großes r in K liegt.
Lösungen. " $\Rightarrow$ " : Wir zeigen zunächst folgende Aussage: Sei $f \in K[X]$ irreduzibel und $r \in \mathbb{N}$ maximal mit der Eigenschaft, dass $f(X) = g(X^{p^r})$ für ein Polynom $g \in K[X]$. Dann ist g durch f eindeutig bestimmt, irreduzibel und separabel.
In der Tat ist es klar, dass g durch die angegebene Beschreibung eindeutig bestimmt ist. Hätte g eine Zerlegung in ein Produkt aus nicht-konstanten Polynomen, dann würden wir durch Einsetzen von X^{p^r} für X eine nichttriviale Zerlegung von f erhalten, was im Widerspruch zur Irreduzibilität von f steht. Wegen der Maximalität von r gibt es einen Koeffizienten $a_n \neq 0$ einer Potenz X^n in g sodass n nicht durch p teilbar ist. Also ist $g' \neq 0$. Nach Satz 3.9.18 ist g also separabel.
Sei jetzt also $\alpha \in L$ und f das Minimalpolynom von α über K. Sei g das zu f gehörige Polynom wie oben, also $f(X) = g(X^{p^r})$ mit $r \in \mathbb{N}$ maximal. Dann ist $\alpha^{p^r} \in L$ eine Nullstelle des separablen, irreduziblen Polynoms g, ist also selbst separabel über K und liegt somit nach Voraussetzung schon in K.

" $\Leftarrow$ " : Sei $\alpha \in L \setminus K$. Dann gibt es also $r \in \mathbb{N}_{>0}$ mit $\alpha^{p^r} \in K$. α ist Nullstelle von $(X - \alpha)^{p^r} = X^{p^r} - \alpha^{p^r} \in K[X]$. Also wird dieses Polynom von $\mathrm{Irr}(\alpha, K)$ geteilt und muss somit α auch als mehrfache Nullstelle haben.

Übungen 6 Lösungen: Algebra und Zahlentheorie

21. Januar 2025

Übung 12.1. Gegeben $n \geq 1$ zeige man, dass $\mathbb{C}(X^n) \subset \mathbb{C}(X)$ eine Galoiserweiterung vom Grad n ist mit zyklischer Galoisgruppe.
Lösung: Schreibe $Y := X^n$. Dann ist X eine Nullstelle von $T^n - Y \in \mathbb{C}(Y)[T]$. Man sieht leicht, dass $T^5 - Y$ in $\mathbb{C}[Y][T]$ und damit nach Gauß auch in $\mathbb{C}(Y)[T]$ irreduzibel ist. Damit ist $\mathbb{C}(X) \supset \mathbb{C}(Y)$ eine algebraische Körpererweiterung von Grad $[\mathbb{C}(X) : \mathbb{C}(Y)] = n$.
Sei nun ζ eine primitive n-te Einheitswurzel in $\mathbb{C}$. Man betrachte dann für $0 \leq i < n$ die Körpermorphismen

$$\begin{aligned} \sigma_i : \mathbb{C}(X) &\to \mathbb{C}(X) \\ X &\mapsto \zeta^i X \end{aligned}$$

Diese fixieren $\mathbb{C}(Y)$, da $\sigma_i(Y) = \sigma_i(X^n) = (\zeta^i X)^n = \zeta^{i \cdot n} X^n = X^n$ und sind injektiv, weil ζ primitiv ist. Damit handelt es sich um n verschiedene Elemente der Galoisgruppe $\mathrm{Gal}(\mathbb{C}(X)/\mathbb{C}(Y))$, und nach Lemma 4.1.4 ist dies bereits die maximale Mächtigkeit, die $\mathrm{Gal}(\mathbb{C}(X)/\mathbb{C}(Y))$ annehmen kann. Nach Satz 4.1.12, 2. $\Rightarrow$ 1. folgt, dass es sich um eine Galoiserweiterung handeln muss.
Weil nach Definition $\sigma_i \circ \sigma_j = (X \mapsto \zeta^{i+j}) = \sigma_{i+j}$ sieht man ebenfalls sofort, dass $\mathrm{Gal}(\mathbb{C}(X)/\mathbb{C}(Y)) \cong \mathbb{Z}/n\mathbb{Z}$, also zyklisch ist.

Übung 12.2. Man bestimme die Galoisgruppe des Zerfällungskörper des Polynoms $X^4 - 5$ über $\mathbb{Q}$ und über $\mathbb{Q}[i]$.
Lösung: $X^4 - 5$ hat die Nullstellen $\pm\sqrt[4]{5}$ und $\pm i\sqrt[4]{5}$. Somit ist der zugehörige Zerfällungskörper $L = \mathbb{Q}(\sqrt[4]{5}, i\sqrt[4]{5}, -\sqrt[4]{5}, -i\sqrt[4]{5}) = \mathbb{Q}(\sqrt[4]{5}, i)$ eine Körpererweiterung von Grad $4 \cdot 2 = 8$.

Betrachte nun die Körpermorphismen τ und σ, wobei τ die komplexe Konjugation sei und σ der Morphismus, der i fixiert und $\sqrt[4]{5}$ auf $i\sqrt[4]{5}$ abbildet. (Man beachte dass dies wohldefiniert ist.)
Nun hat τ Ordnung 2 und σ Ordnung 4 und durch Nachrechnen kann man sich davon überzeugen, dass $\tau \circ \sigma \circ \tau = \sigma^{-1}$. Das bedeutet, dass die von τ und σ erzeugte Gruppe der Diedergruppe D_4 entspricht. Diese hat 8 Elemente und ist somit bereits die gesamte Galoisgruppe. Insbesondere handelt es sich um eine Galoiserweiterung.
Es gilt also $\mathrm{Gal}(L/\mathbb{Q}) = \langle \tau, \sigma \rangle \cong D_4$.
Die Gruppe $\mathrm{Gal}(L/\mathbb{Q}(i))$ ist nun genau die Untergruppe von $\langle \tau, \sigma \rangle$, die $\mathbb{Q}(i)$, also insbesondere i fixiert. Diese muss Index 2 haben, da $[\mathbb{Q}(i) : \mathbb{Q}] = 2$.
Per Definition ist $\sigma(i) = i$, also ist $\langle \sigma \rangle \cong C_4$ genau die gesuchte Untergruppe.

Übung 12.3. Man zeige: Gegeben eine endliche Galoiserweiterung L/K ist die ***Spurabbildung*** $S_L^K : L \to K$ *gegeben durch*

$$x \mapsto \sum_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x)$$

eine K-lineare von Null verschiedene Abbildung und die ***Spurform*** $L \times L \to K$ *gegeben durch $(x, y) \mapsto S_L^K(xy)$ ist eine nichtausgeartete Bilinearform auf dem K-Vektorraum L. Hinweis: Lineare Unabhängigkeit von Charakteren.*
Lösung: Das Bild von S_L^K liegt in K, da Elemente aus dem Bild per Konstruktion von allen Elementen aus $\mathrm{Gal}(L/K)$ fixiert werden. (Anwendung eines $\sigma \in \mathrm{Gal}(L/K)$ führt lediglich zu einer Permutation der Summe.)
S_L^K ist K-linear, denn für $x, y \in L, \lambda \in K$ gilt

$$\begin{aligned} S_L^K(\lambda x + y) &= \sum_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\lambda x + y) \\ &= \sum_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\lambda)\sigma(x) + \sigma(y) \\ &= \lambda \sum_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x) + \sum_{\sigma \in \mathrm{Gal}(L/K)} \sigma(y) \\ &= \lambda S_L^K(x) + S_L^K(y) \end{aligned}$$

Dabei gilt die zweite Gleichheit, da σ Körpermorphismus ist und die dritte, da σ K fixiert.
Damit ist die angegebene Spurform $L \times L \to K$ mit $(x, y) \mapsto S_L^K(xy)$ auch

eine Bilinearform, welche nicht ausgeartet ist, solange S_L^K nicht die Nullabbildung ist.
Um zu zeigen, dass $S_L^K \neq 0$, kann man Satz 3.8.15 (Lineare Unabhängigkeit von Charakteren) verwenden: Alle $\sigma \in \mathrm{Gal}(L/K)$ sind insbesondere Homomorphismen von $L^\times \to L^\times$ und damit linear unabhängig im Vektorraum aller Abbildungen $L^\times \to L$. Damit muss jede nicht triviale Linearkombination der $\sigma \in \mathrm{Gal}(L/K)$ und damit insbesondere S_L^K ungleich Null sein.

Übung 12.4. Sei k ein Körper der Charakteristik $p > 0$ und $\lambda \in k^\times$ und $t = t_\lambda : k(X) \xrightarrow{\sim} k(X)$ der Körperautomprphismus über k mit $X \mapsto X + \lambda$. Man zeige, dass der Körper der Invarianten genau das Bild derjenigen Einbettungen $k(Y) \hookrightarrow k(X)$ ist, die durch $Y \mapsto X^p - \lambda^{p-1}X$ gegeben wird.
Lösung: Zunächst überprüfe ich, dass $k(Y)$ tatsächlich von t_λ fixiert wird:

$$t_\lambda(X^p - \lambda^{p-1}X) = (X+\lambda)^p - \lambda^{p-1}(X+\lambda) = X^p + \lambda^p - \lambda^{p-1}X - \lambda^p = X^p - \lambda^{p-1}X$$

Es bleibt nun zu zeigen, dass es keinen größeren Körper $k(Y) \subsetneq L \subseteq k(X)$ gibt, der von t_λ fixiert wird.
Dies geht mit folgender Beobachtung: Da in Charakteristik p gilt, dass $n^{p-1} = 1$ für alle $n \in \{0, 1, \ldots, p-1\}$, wird $k(Y)$ mit der gleichen Rechnung auch von allen $t_{n\lambda}$ fixiert.
Also hat $\mathrm{Gal}(k(X)/k(Y))$ mindestens p verschiedene Elemente und damit $[k(X) : k(Y)] \geq p$. Da aber X Nullstelle ist von $T^p - \lambda^{p-1}T - Y \in k(Y)[T]$, muss der Grad sogar genau p sein. Da p prim ist, kann es (wegen Multiplikativität des Grades) keine Körper zwischen $k(Y)$ und $k(X)$ geben. Da $k(X)$ offensichtlich nicht von t_λ fixiert wird, muss also $k(Y)$ genau der Körper der Invarianten von t_λ sein.

Übungen 13 Lösungen: Algebra und Zahlentheorie

Übung 13.1. Man zeige: Gegeben eine Körpererweiterung L/K und zwei verschiedene normierte irreduzible Polynome in $K[X]$ kann kein Element der Galoisgruppe eine Nullstelle des einen Polynoms in eine Nullstelle des anderen Polynoms überführen.

Lösungen. This follows easily from the fact that the minimal polynomial of an element of L is unique (if it exists). Explicitly, let $\alpha \in L$ be algebraic over K, and let f be its minimal polynomial in $K[X]$. Let $\sigma \in \mathrm{Aut}(L/K)$. Then $\sigma(\alpha)$ is a root of $\sigma(f) = f$, so f is also the minimal polynomial of $\sigma(\alpha)$. The result follows.

Übung 13.2. Wieviele zu 140000 teilerfremde Zahlen a mit $1 \leq a \leq 140000$ gibt es?

Lösungen. We decompose $140000 = 2^5 * 5^4 * 7$. There are 70000 (resp. 28000, 20000, 14000, 10000, 4000, 2000) integers less than or equal to 140000 that are divisible by 2 (resp. 5, 7, 10, 14, 35, 70). So the number of a which are coprime to and no larger than 140000, equals

$$140000 - (70000 + 28000 + 20000) + (14000 + 10000 + 4000) - 2000 = 48000.$$

by the inclusion-exclusion principle.

Übung 13.3. Man zeige, daß die Einheitswurzeln des n-ten Kreisteilungskörpers für gerades n genau die n-ten Einheitswurzeln sind und für ungerades n genau die $2n$-ten Einheitswurzeln.

Lösungen. Consider the n'th cyclotomic field $\mathbb{Q}(\zeta_n)$, where $\zeta_n = e^{2i\pi/n}$ is a primitive n'th root of unity of $\mathbb{C}$. Let R be the group of roots of unity of $\mathbb{Q}(\zeta_n)$. Suppose R is infinite. Then one can find arbitrarily large m such that $\zeta_m \in \mathbb{Q}(\zeta_n)$. The degree of ζ_m goes to ∞ as $m \to \infty$, so we can find elements in $\mathbb{Q}(\zeta_n)$ of arbitrarily large degree over $\mathbb{Q}$. This contradicts the fact that $\mathbb{Q}(\zeta_n)$ is an algebraic number field, so R is finite. Recall that every finite subgroup of the group of units of a field is cyclic. Hence R is cyclic.

Let $r := |R|$. Clearly n divides r, say $r = nl$ for some l.

Since $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_r)$, a consideration of degrees over $\mathbb{Q}$ shows that $\varphi(n) = \varphi(r)$. We need the following identity for the Euler function: $\varphi(ab) \geq \varphi(a)\varphi(b)$ for all positive integers a, b, with equality if and only if $gcd(a, b) = 1$. Applying this gives us

$$\varphi(n) = \varphi(r) = \varphi(nl) \geq \varphi(n)\varphi(l).$$

Hence $\varphi(l) \leq 1$, so $l = 1$ or 2. If n is odd then $-\zeta_n \in R$ has order $2n$, and hence $l = 2$. If n is even then $l = 1$, as otherwise $gcd(l, n) \neq 1$ and so $\varphi(l) < 1$ (a contradiction).

Übung 13.4. Gegeben $n > 2$ zeige man, daß im Kreisteilungskörper $\mathbb{Q}(\sqrt[n]{1}) = \mathbb{Q}(\zeta)$ für ζ eine primitive n-te Einheitswurzel gilt $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})] = 2$ und $[\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}] = \varphi(n)/2$. Man folgere $\Phi_n(X) = X^{\varphi(n)}\Phi_n(X^{-1})$.

Lösungen. Since ζ is a root of the polynomial

$$(X - \zeta)(X - \zeta^{-1}) = X^2 - (\zeta + \zeta^{-1})X + 1 \in \mathbb{Q}(\zeta + \zeta^{-1})[X],$$

we see that $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})] \leq 2$. Observe that $\zeta + \zeta^{-1} \in \mathbb{R}$, but $\zeta \notin \mathbb{R}$. Hence $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})] = 2$.

We saw in class that $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$. Then

$$\varphi(n) = [\mathbb{Q}(\zeta) : \mathbb{Q}] = [\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})][\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}],$$

so indeed $[\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}] = \varphi(n)/2$.

There are several ways to prove the final assertion, my favourite is as follows. We recall that the cyclotomic polynomial $\Phi_n(X)$ is monic, irreducible, has degree $\varphi(n)$, and has root ζ. Clearly $X^{\varphi(n)}\Phi_n(X^{-1})$ has degree $\varphi(n)$ and it has ζ as a root – hence it is irreducible. Since $n > 2$, 1 and -1 are not roots of $\Phi_n(X)$, so every root may be paired with its (distinct) inverse. So the constant term of $\Phi_n(X)$ is 1. Hence $X^{\varphi(n)}\Phi_n(X^{-1})$ is monic. Then we

are done, as a monic irreducible polynomial is uniquely determined by one of its roots.