Übungsblatt 11: Galoistheorie

1. Galoiskorrespondenz

S 1.1. (12 Punkte) In der Aufgabe 3.3 auf Blatt 10 wurde gezeigt, dass das Polynom X^4-2 den Zerfällungskörper $E=\mathbb{Q}[i,\sqrt[4]{2}]$ über $\mathbb{Q}$ besitzt und $|E:\mathbb{Q}|=8$ gilt.

(a) Die komplexe Konjugation induziert $\sigma\in\mathrm{Aut}(E|\,\mathbb{Q})$ der Ordnung 2.

(b) Man zeige $|E:\mathbb{Q}[i]|=4$ und bestimme $\rho\in\mathrm{Aut}(E|\,\mathbb{Q}[i])$ der Ordnung 4. *Hinweis:* Satz 12D6 oder Aufgabe 3.3.

(c) Man bestimme eine Basis und alle Automorphismen von $E|\,\mathbb{Q}$.

Das zeigt, dass E galoissch über $\mathbb{Q}$ ist.

Die Nullstellenmenge von X^4-2 ist $M=\{\pm\sqrt[4]{2},\pm i\sqrt[4]{2}\}$.

(d) Geben Sie die Wirkung von $\mathrm{Aut}(E|\,\mathbb{Q})$ auf M in einer Tabelle an. Ist $\mathrm{Aut}(E|\,\mathbb{Q})$ isomorph zur Diedergruppe D_4 der Ordnung 8?

(e) Man bestimme alle Untergruppen von $\mathrm{Aut}(E|\,\mathbb{Q})$. (Es sind 10 Stück.)

(f) Bestimmen Sie alle Zwischenkörper der Erweiterung $\mathbb{Q}[\sqrt[4]{2},i]\mid\mathbb{Q}$.

V 1.2. Sei $E|K$ eine Galoiserweiterung. Seien F und F' Zwischenkörper von $E|K$ und seien $H=\mathrm{Aut}(E|\,F)$ und $H'=G(E|F')$ die zugehörigen Untergruppen von $\mathrm{Aut}(E|\,K)$. Sei $U=\langle H,H'\rangle$ die von H und H' erzeugte Untergruppe. Zeigen Sie

$$\mathrm{Fix}(U)=F\cap F'.$$

Dual hierzu: Zeigen Sie

$$\mathrm{Fix}(H\cap H')=FF'.$$

Hierbei ist $FF'=F(F')=F'(F)$.

2. Gegenbeispiele

V 2.1. Zeigen Sie, dass $\mathbb{Q}[\sqrt[4]{2}]$ galoisch über $\mathbb{Q}[\sqrt{2}]$ und $\mathbb{Q}[\sqrt{2}]$ galoisch über $\mathbb{Q}$ ist, aber $\mathbb{Q}[\sqrt[4]{2}]$ nicht galoisch über $\mathbb{Q}$ ist.

2.2. Man betrachte den Körper $E=\mathbb{F}_p(T)$ und den Teilkörper $K=\mathbb{F}_p(T^p)$. Bestimmen Sie das Minimalpolynom von T über K. Warum ist $E|K$ nicht separabel?

2.3. Bestimmen Sie $\mathrm{Aut}(\mathbb{Q}[\sqrt[3]{2}]\mid\mathbb{Q})$. Ist $\mathbb{Q}[\sqrt[3]{2}]\mid\mathbb{Q}$ eine Galoiserweiterung?

3. Verschiedenes

3.1. Man bestimme die Minimalpolynome von $\sqrt{2}+\sqrt{3}$ und $\sqrt{2+\sqrt[3]{2}}$ über $\mathbb{Q}$.

V 3.2. Sei $p\in\mathbb{N}$ eine Primzahl und $\xi=e^{2\pi i/p}$ eine p-te Einheitswurzel in $\mathbb{C}$. Man bestimme das Minimalpolynom $\mathrm{Irr}^X_{\mathbb{Q}}(\xi)$ und alle seine Wurzeln in $\mathbb{C}$. Hieraus gewinne man einen Gruppenisomorphismus $\mathbb{Z}/_p^{\times}\xrightarrow{\sim}\mathrm{Aut}(\mathbb{Q}[\xi]\mid\mathbb{Q})$.

3.3. Sei K ein Körper und $f\in K[X]$ ein nicht-konstantes Polynom dessen Nullstellen alle einfach seien. Sei E ein Zerfällungskörper von f über K. Es sind äquivalent:

(1) Das Polynom $f\in K[X]$ ist irreduzibel.

(2) Die Gruppe $\mathrm{Aut}(E|\,K)$ operiert transitiv auf den Nullstellen von f, d.h. zu je zwei Nullstellen $a,b\in E$ von f existiert ein $\sigma\in\mathrm{Aut}(E|\,K)$, so dass $\sigma(a)=b$.

Hinweis: Sätze 12D6 und 12D12.

4. Fehlererkennende und fehlerkorrigierende Codes

Ein *Bit* ist die minimale Informationseinheit $a \in \{0,1\}$. Wir identifizieren das Alphabet $\{0,1\}$ mit dem Körper $\mathbb{F}_2$. Eine Folge $(a_{n-1},\dots,a_1,a_0)$ von n Bits betrachten wir als Polynom $\sum_{i=0}^{n-1} a_k X^k$ in $\mathbb{F}_2[X]_{<n}$.

Fehlererkennender Code. — Ein Sender möchte eine Nachricht $P \in \mathbb{F}_2[X]_{<n}$ von n Bits über einen fehlerbehafteten Kanal übermitteln. Das benutzte Protokoll soll dem Empfänger erlauben einen eventuell auftretenden Bitfehler *erkennen* zu können. Statt P übermittelt man hierzu eine Nachricht $T \in \mathbb{F}_2[X]_{<m}$. Die empfangene Nachricht T^* ist bei fehlerfreier Übermittlung gleich T. Wird das i-te Bit von T fehlerhaft übermittelt, dann gilt $T^* = T + X^i$ mit $0 \leq i < m$. (Wir nehmen an, dass höchstens ein Bitfehler vorliegt.)

4.1. Eine einfache Methode den Fehler zu erkennen, besteht darin, die Nachricht $P \in \mathbb{F}_2[X]_{<n}$ zweimal zu übermitteln. (Das kostet $2n$ Bits.) Statt P übermittelt man also die Nachricht $T = X^n P + P$ in $\mathbb{F}_2[X]_{<2n}$. Man erkläre, wie dieses Protokoll die Erkennung eines Bitfehlers ermöglicht. Ermöglicht es auch seine Korrektur?

4.2. Man kann die Nachricht $P \in \mathbb{F}_2[X]_{<n}$ auch mit einem *Paritätsbit* versehen: Dies ist die Quersumme $P(1) = a_{n-1} + \cdots + a_0 \in \mathbb{F}_2$. Das so ergänzte Polynom $Q = XP + P(1)$ in $\mathbb{F}_2[X]_{<n+1}$ erfüllt stets $Q(1) = 0$. Man erläutere, wie die Übermittlung dieser $n+1$ Bits die Erkennung eines Bitfehlers ermöglicht. Ermöglicht sie auch seine Korrektur?

Fehlerkorrigierender Code. — Ein Sender möchte 120 Bits über einen fehlerbehafteten Kanal übermitteln. Dieses Mal wollen wir ein eventuell auftretendes fehlerhaftes Bit nicht nur erkennen, sondern auch *korrigieren* können.

4.3. Eine einfache Methode besteht darin, die Nachricht 3 mal nacheinander zu übermitteln. (Das kostet 360 Bits.) Man erkläre, wie dies die Korrektur eines Bits ermöglicht.

4.4. Eine etwas bessere Methode besteht darin, die Nachricht $P \in \mathbb{F}_2[X]_{<120}$ mit einem Paritätsbit versehen und $Q = XP + P(1)$ zweimal zu übermitteln. (Das kostet 242 Bits.) Man erkläre, wie dieses Protokoll die Korrektur eines Bitfehlers erlaubt.

Damit haben wir die Kosten bereits von 360 Bit auf 242 Bit gesenkt. Wir präsentieren schließlich eine dritte, noch raffiniertere Methode. Für dieses Protokoll wählen wir ein irreduzibles Polynom $A \in \mathbb{F}_2[X]$ vom Grad 7. Ist $P \in \mathbb{F}_2[X]_{<120}$ die zu übermittelnde Nachricht, so berechnen wir $R = X^7 P \mod A$ und setzen $T = X^7 P + R$ in $\mathbb{F}_2[X]_{<127}$.

4.5. Die gesendete Nachricht erfüllt die Bedingung $T \mod A = 0$. Sei $T^* = T + X^i$ die empfangene Nachricht, wobei $0 \leq i < 127$. Im Körper $F = \mathbb{F}_2[X]/(A)$ sei x das Bild von X. Man zeige, dass x die Gruppe $F^\times$ erzeugt. Die Abbildung $X^i \mapsto x^i$ ist also injektiv für $0 \leq i < 127$. Man erkläre, wie man die ursprüngliche Nachricht T aus der empfangenen Nachricht T^* rekonstruieren kann. Worin besteht der Vorteil dieser Methode?

4.6. Um das obige Protokoll wirklich zu implementieren, müssen sich Sender und Empfänger vorab auf ein irreduzibles Polynom $A \in \mathbb{F}_2[X]$ vom Grad 7 verständigen. Wir schlagen $A = X^7 + X^3 + 1$ vor. Man zeige, dass A irreduzibel ist.
Hinweis: Man erstelle zunächst die Liste aller irreduziblen Polynome vom Grad ≤ 3 in $\mathbb{F}_2[X]$. Diese sind X, $X+1$, X^2+X+1, X^3+X^2+1, X^3+X+1.