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 $\mathbb{Q}[\sqrt[4]{2},i]\mid\mathbb{Q}$.

Lösungshinweise: —

(a) *Die komplexe Konjugation bildet die Menge der Nullstellen $\pm\sqrt[4]{2},\pm i\sqrt[4]{2}$ auf sich selbst ab und somit den Zerfällungskörper E (surjektiv) auf sich. Die Automorphismuseigenschaft folgt nun daraus, dass σ in $\mathbb{C}$ ein Automorphismus ist.*

(b) *Nach Gradformel ist* $8=|E:\mathbb{Q}|=|E:\mathbb{Q}[i]|\cdot|\mathbb{Q}[i]:\mathbb{Q}|$. *Aus* $|\mathbb{Q}[i]:\mathbb{Q}|=2$ *folgt dann* $|E:\mathbb{Q}[i]|=4$. *Die Automorphismengruppe* $\mathrm{Aut}(E|\,\mathbb{Q}[i])$ *kann also nach dem Satz von Galois höchstens* 4 *Elemente haben und diese wollen wir nun bestimmen. Das Polynom X^4-2 ist irreduzibel über $\mathbb{Q}[i]$, da $X^4-2=X^4-(1+i)(1-i)$ in $\mathbb{Z}[i]$ nach Eisenstein (zum Primelement $1+i$) irreduzibel ist. Damit kann man Satz 12D6 anwenden, der sagt, dass man einen Automorphismus ρ von $E=\mathbb{Q}[i][i\sqrt[4]{2}]$ über $K=\mathbb{Q}[i]$ mit $\tau(\sqrt[4]{2})=i\sqrt[4]{2}$ findet. Es ist dann $\rho(i\sqrt[4]{2})=\rho(i)\rho(\sqrt[4]{2})=i\cdot i\sqrt[4]{2}=-\sqrt[4]{2}\neq\sqrt[4]{2}$ und somit hat ρ Ordnung* 4.

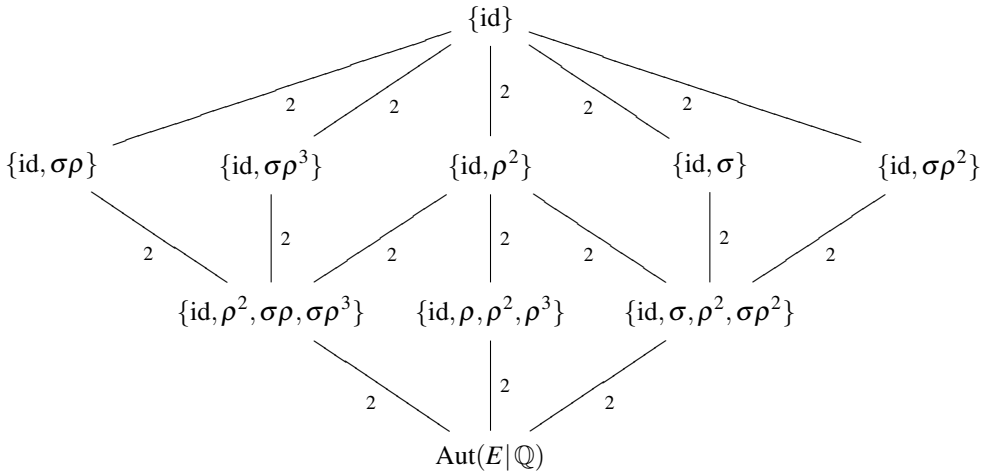
(c) *Eine Basis ist gegeben durch* $\{1,\sqrt[4]{2},\sqrt{2},\sqrt[4]{8},i,i\sqrt[4]{2},i\sqrt{2},i\sqrt[4]{8}\}$ *(siehe Aufgabe 3.3 auf Blatt 10). Betrachtet man die Menge, der von σ und ρ erzeugten Automorphismen, so ergibt sich* $\{\mathrm{id},\rho,\rho^2,\rho^3,\sigma,\sigma\rho,\sigma\rho^2,\sigma\rho^3\}$. *Dies müssen schon alle sein, da* $|\mathrm{Aut}(E|\,\mathbb{Q})|\leq|E:\mathbb{Q}|=8$ *und die Abbildungen alle verschieden sind, wie man durch einsetzen der Basiselemente nachprüft.*

(d) *Die folgende Tabelle zeigt uns noch einmal, dass alle* 8 *Automorphismen in der Liste verschieden sind, weil sie alle unterschiedlich auf der Nullstellenmenge operieren.*

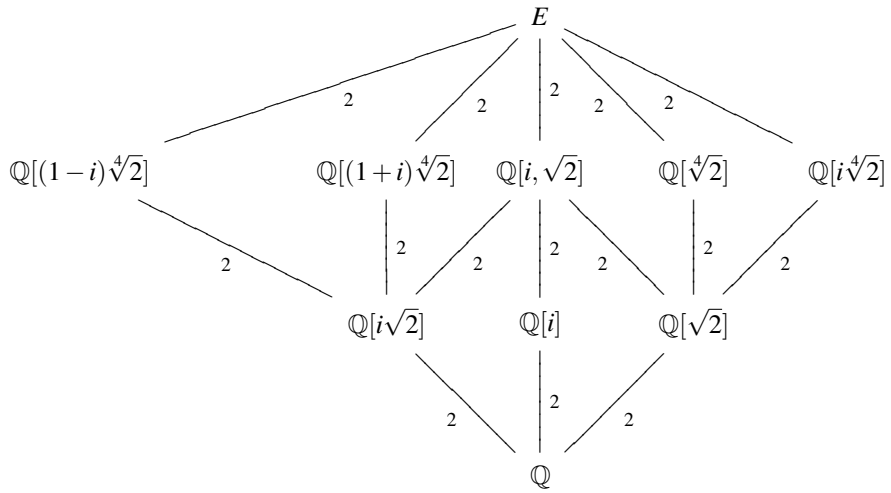
id	ρ	ρ^2	ρ^3	σ	$\sigma\rho$	$\sigma\rho^2$	$\sigma\rho^3$
$\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$-i\sqrt[4]{2}$	$\sqrt[4]{2}$	$-i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$i\sqrt[4]{2}$
$i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$-i\sqrt[4]{2}$	$\sqrt[4]{2}$	$-i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$i\sqrt[4]{2}$	$\sqrt[4]{2}$
$-\sqrt[4]{2}$	$-i\sqrt[4]{2}$	$\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$i\sqrt[4]{2}$	$\sqrt[4]{2}$	$-i\sqrt[4]{2}$
$-i\sqrt[4]{2}$	$\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$i\sqrt[4]{2}$	$\sqrt[4]{2}$	$-i\sqrt[4]{2}$	$-\sqrt[4]{2}$

Betrachtet man die Menge der Nullstellen als Quadrat in $\mathbb{C}$, so operiert ρ darauf wie eine Drehung um 90 *Grad und σ wie eine Spiegelung an einer Diagonalen. Die Gruppe ist also isomorph zur D_4. Dies sieht man aber auch schon daran, dass sie isomorph zu einer Untergruppe der $S_M\cong S_4$ von Ordnung* 8 *ist, welche nach Sylowsatz konjugiert zur D_4 sein muss.*

(e) *Für den Untergruppenverband erhält man:*



(f) *Um die zugehörigen Zwischenkörper zu finden, muss man schauen, was von den einzelnen Automorphismen festgehalten wird. Wir setzen dazu beispielsweise eine allgemeine Linearkombination* $a+b\sqrt[4]{2}+c\sqrt{2}+d\sqrt[4]{8}+ei+fi\sqrt[4]{2}+gi\sqrt{2}+hi\sqrt[4]{8}$ *an und wenden die Homomorphismen darauf an. Manchmal können auch Dimensionsargumente helfen. Damit erhält man schon die meisten Einträge im unteren Diagramm. Am schwierigsten sind die beiden Körper zu den Gruppen* $\{\mathrm{id},\sigma\rho\}$ *und* $\{\mathrm{id},\sigma\rho^3\}$ *zu finden. Es ist* $\sigma\rho(a+b\sqrt[4]{2}+c\sqrt{2}+d\sqrt[4]{8}+ei+fi\sqrt[4]{2}+gi\sqrt{2}+hi\sqrt[4]{8}) = a-bi\sqrt[4]{2}-c\sqrt{2}+di\sqrt[4]{8}-ei-f\sqrt[4]{2}+gi\sqrt{2}+h\sqrt[4]{8}$*. Soll das Element fest bleiben, so folgt daraus* $b=-f, c=-c, d=h, e=-e$*, also hat das Element die Form* $a+b(\sqrt[4]{2}-i\sqrt[4]{2})+gi\sqrt{2}+d(\sqrt[4]{8}+i\sqrt[4]{8})$*. Damit sieht man (aus Dimensionsgründen), dass der Körper von dem Element* $\sqrt[4]{2}-i\sqrt[4]{2}$ *erzeugt wird und somit erhalten wir* $\mathrm{Fix}(\{\mathrm{id},\sigma\rho\}) = \mathbb{Q}[\sqrt[4]{2}-i\sqrt[4]{2}]$ *und ebenso erhält man* $\mathrm{Fix}(\{\mathrm{id},\sigma\rho^3\}) = \mathbb{Q}[\sqrt[4]{2}+i\sqrt[4]{2}]$.



—

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

Lösungshinweise: — *Die von H und H' erzeugte Untergruppe hält alles in $F \cap F'$ fest, weil jedes Element aus H und H' es tut. Andererseits gibt es zu $z' \in F' \setminus F$ ein $h \in H$ mit $h(z') \neq z'$. Andernfalls wäre $F = \mathrm{Fix}(H) \supset F[z'] \supset F$, also $z' \in F$. Damit ist also $z' \notin \mathrm{Fix}(U)$, was zu zeigen war. Symmetrisch dazu folgt das auch für $z \in F \setminus F'$.*
Für die zweite Aussage sehen wir, dass alle Elemente in $H \cap H'$ sowohl F, als auch F' festhalten und damit auch den davon erzeugten Unterkörper FF'. Ein Element $g \in \mathrm{Aut}(E|K)$, das FF' punktweise festhält, hält insbesondere die Teilmengen F und F' fest, ist also in H und H' enthalten und somit in $H \cap H'$. —

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.

Lösungshinweise: — *Man sieht mit Aufgabe 4.5 vom Blatt 10, dass $\mathrm{Fix}(\mathrm{Aut}(\mathbb{Q}[\sqrt{2}]|\mathbb{Q})) = \mathbb{Q}$, so dass diese Erweiterung galoissch ist.*
Jeder Automorphismus σ von $\mathbb{Q}[\sqrt[4]{2}]$ über $\mathbb{Q}$ und über $\mathbb{Q}[\sqrt{2}]$ schickt $\sqrt[4]{2}$ auf eine Nullstellen $\pm\sqrt[4]{2}$ von X^4-2, die in $\mathbb{Q}[\sqrt[4]{2}]$ liegen. Damit ist aber stets $\sigma(\sqrt{2}) = \sigma(\sqrt[4]{2})^2 = \sqrt{2}$. Also ist $\mathrm{Fix}(\mathrm{Aut}(\mathbb{Q}[\sqrt[4]{2}]|\mathbb{Q}[\sqrt{2}])) \supset \mathbb{Q}[\sqrt{2}]$ und $\mathrm{Fix}(\mathrm{Aut}(\mathbb{Q}[\sqrt[4]{2}]|\mathbb{Q})) \supset \mathbb{Q}[\sqrt{2}]$. Die dritte Erweiterung ist also schon mal nicht galoissch.
Nach Aufgabe 4.5 vom Blatt 10 ist der Automorphismus σ von $\mathbb{Q}[\sqrt[4]{2}]|\mathbb{Q}[\sqrt{2}]$ mit $\sigma(\sqrt[4]{2}) = -\sqrt[4]{2}$ nichttrivial und hält gerade $\mathbb{Q}[\sqrt{2}]$ fest, so dass $\mathrm{Fix}(\mathrm{Aut}(\mathbb{Q}[\sqrt[4]{2}]|\mathbb{Q}[\sqrt{2}])) = \mathbb{Q}[\sqrt{2}]$ gilt. Die Erweiterung ist also galoissch. Damit haben wir gezeigt, dass die Eigenschaft "galoissch" zu sein bei Körpererweiterungen nicht transitiv 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?

Lösungshinweise: — *Das Minimalpolynom ist $X^p - T^p$ und ist über $\mathbb{F}_p[T^p]$ nach Eisenstein irreduzibel und damit auch über $K = \mathbb{F}_p(T^p)$. In $E = \mathbb{F}_p(T)$ zerfällt es allerdings in $X^p - T^p = (X-T)^p$ und hat die p-fache Nullstelle T. Das zeigt, dass $E|K$ nicht separabel ist, da das Minimalpolynom des Elementes T mehrfache Nullstellen besitzt.* —

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?

Lösungshinweise: — *Da X^3-2, das Minimalpolynom über $\mathbb{Q}$ von $\sqrt[3]{2}$, nur eine reelle Nullstelle in $\mathbb{Q}[\sqrt[3]{2}]$ besitzt, kann diese nur auf sich selbst abgebildet werden. Damit ist aber jeder Automorphismus die Identität und es gilt $\mathrm{Fix}(\mathrm{Aut}(\mathbb{Q}[\sqrt[3]{2}] \mid \mathbb{Q})) = \mathbb{Q}[\sqrt[3]{2}]$. Damit ist die Erweiterung nicht galoissch.* —

3. Verschiedenes

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

Lösungshinweise: — *Man berechnet die sukzessiven Potenzen des Elementes $x = \sqrt{2}+\sqrt{3}$: $1, \sqrt{2}+\sqrt{3}, 5+2\sqrt{6}, 11\sqrt{2}+9\sqrt{3}, 49+20\sqrt{6}$. Hier sieht man dann, dass die vierte Potenz durch die anderen über $\mathbb{Q}$ linear kombiniert werden kann: $x^4 = 49+20\sqrt{6} = 10x^2-1$. Das Polynom $P(X) = X^4 - 10X^2 + 1$ ist irreduzibel (sieht man z.B. mit der Ansatzmethode) und somit das Minimalpolynom der Nullstelle $\sqrt{2}+\sqrt{3}$. Bei dem zweiten Element $y = \sqrt{2+\sqrt[3]{2}}$ sieht man direkt, dass $(y^2-2)^3 - 2 = 0$ gilt. Es ist also Nullstelle*

des Polynoms $Y^6 - 6Y^4 + 12Y^2 - 10$. Dieses ist auch irreduzibel (Eisenstein zu $p = 2$) und somit das Minimalpolynom. —

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 $\operatorname{Irr}^X_{\mathbb{Q}}(\xi)$ und alle seine Wurzeln in $\mathbb{C}$. Hieraus gewinne man einen Gruppenisomorphismus $\mathbb{Z}/_p^\times \xrightarrow{\sim} \operatorname{Aut}(\mathbb{Q}[\xi] \mid \mathbb{Q})$.

Lösungshinweise: — *ξ ist Nullstelle des Polynoms $X^p - 1$ und somit ist das Minimalpolynom ein Teiler von $X^p - 1 = (X-1)(X^{p-1} + \ldots + 1)$. Der zweite Faktor liegt in $\mathbb{Q}[X]$, ist nach Vorlesung irreduzibel und somit das Minimalpolynom von ξ über $\mathbb{Q}$.*
Die Potenzen ξ^k für $0 \le k \le p-1$ sind p verschiedene Nullstellen von $X^p - 1$. Damit sind die Potenzen ξ^k für $1 \le k \le p-1$ die anderen gesuchten Nullstellen.
Nach Satz 12D6 gibt es Automorphismen σ_i, die ξ auf die $p-1$ verschiedenen Nullstellen ξ^i abbilden. Damit ist aber wegen $\sigma_i(\xi^k) = \sigma_i(\xi)^k$ der Automorphismus schon festgelegt. Wir haben also eine injektive Abbildung $\varphi : \mathbb{Z}/_p^\times \to \operatorname{Aut}(\mathbb{Q}[\xi]|\mathbb{Q}) : i \mapsto \sigma_i$. Es ist weiter $\varphi(ij)(\xi) = \sigma_{ij}(\xi) = \xi^{ij} = (\xi^j)^i = \sigma_i(\sigma_j(\xi)) = \varphi(i) \circ \varphi(j)(\xi)$. Damit ist φ ein injektiver Gruppenhomomorphismus. Wegen $|\operatorname{Aut}(\mathbb{Q}[\xi]|\mathbb{Q})| = \deg(Irr^x_{\mathbb{Q}}(\xi)) = p-1$ ist dieser auch surjektiv. —

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 $\operatorname{Aut}(E|K)$ operiert transitiv auf den Nullstellen von f, d.h. zu je zwei Nullstellen $a, b \in E$ von f existiert ein $\sigma \in \operatorname{Aut}(E|K)$, so dass $\sigma(a) = b$.
Hinweis: Sätze 12D6 und 12D12.

Lösungshinweise: — *(1) $\Rightarrow$ (2): Da f irreduzibel ist, so folgt aus Satz 12D6, dass es einen Isomorphismus φ von $K[a]$ nach $K[b]$ mit $\varphi(a) = b$. und $\varphi|_K = \mathrm{id}$. Dieser lässt sich nach 12D12 zu einem Automorphismus $\sigma : E \to E$ fortsetzen, da a und b dasselbe Minimalpolynom und somit denselben Zerfällungskörper haben.*
(2) $\Rightarrow$ (1): Ist f reduzibel, so betrachte zwei verschiedene irreduzible Komponenten g und h von f. Jeder Automorphismus bildet Nullstellen von g auf Nullstellen von g ab und Nullstellen von h auf Nullstellen von h. Da alle Nullstellen einfach sind, haben g und h keine gemeinsamen Nullstellen und somit gibt es keinen Automorphismus, der eine Nullstelle a von g auf eine Nullstelle b von h abbildet. Somit operiert $\operatorname{Aut}(E|K)$ nicht transitiv. —

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 $(a_{n-1}, \ldots, a_1, a_0)$ 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 $0 \le i < m$. (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?

Lösungshinweise: — *Sei $T^* = P'X^n + P''$ Man berechne $T^* \mod (X^n - 1)$ und erhält $P' + P''$. Wenn man 0 erhält, hat es keinen Bitfehler gegeben. Sonst erhält man X^i mit der Fehlerstelle i oder $i+n$. Man kann den Fehler allerdings nicht korrigieren, da man nicht weiß, welche der beiden Stellen nun wirklich betroffen war.* —

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?

Lösungshinweise: — *Ändert sich ein Bit in Q^*, so wird $Q^*(1) = 1$ und man erkennt, dass ein Fehler stattgefunden hat, weiß nun aber überhaupt nicht mehr an welcher Stelle. Dafür benötigte man aber auch nur $n+1$ statt $2n$ Bits.* —

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.

Lösungshinweise: — *Man übermittelt $T = PX^{2n} + PX^n + P$ in $\mathbb{F}_2[X]_{<3n}$. Man vergleiche die Werte an den Stellen $i, i+n, i+2n$. Sind alle drei gleich, so hat es keinen Fehler gegeben. Wenn nur zwei übereinstimmen, so wissen wir (da es nach Annahme nur einen Bitfehler gab), dass diese beiden den korrekten Wert und die dritte Stelle den fehlerhaften Wert anzeigt. Damit kann nun die ursprüngliche Nachricht rekonstruiert werden.* —

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.

Lösungshinweise: — *Man sendet also $T = QX^{n+1} + Q$ ab. Wenn $T^* = Q'X^n + Q''$, so gilt, dass $Q'(1) = 0$ oder $Q''(1) = 0$ Daraus kann man feststellen, welche die richtige Nachricht ist und diese liefert P zurück.* —

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?

Lösungshinweise: — *Die Gruppe $F^\times$ ist nach Vorlesung zyklisch und hat* 127 *Elemente.* 127 *ist eine Primzahl und damit ist nach Lagrange jedes Element ein Erzeuger, also auch x. Insbesondere sind alle x^i $0 \leq i < 127$ verschieden.*
Es sei $T^* = T + X^i$ und damit $T^* \mod A = X^i \mod A \neq 0$. Da die Abbildung $X^i \mapsto x^i$ für $0 \leq i < 127$ nach Vorüberlegung injektiv ist, kann man X^i und somit i als Urbild zurückgewinnen (z.B. durch eine Tabelle aller Werte). Damit kann $T = T^* - X^i$ wiedergewonnen werden.
Wir haben dabei insgesamt nur 128 *Bits zur Übermittlung von* 120 *Bits gebraucht.* —

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.

Lösungshinweise: — *Ein reduzibles Polynom vom Grad* 7 *muss einen Faktor von Grad ≤ 3 besitzen. Probiert man aber alle solchen Polynome durch, so sieht man, dass dies nicht der Fall ist und somit ist A irreduzibel.* —