Musterlösung 21

Endliche Körper

1. Finde für $p^r = 8$, 9, 16 das Minimalpolynom über $\mathbb{F}_p$ eines Erzeugenden von $\mathbb{F}_{p^r}^\times$.

   Lösung: Sei $p^r = 8$. Dann ist $\mathbb{F}_8$ isomorph zu $\mathbb{F}_2[X]/(X^3+X+1)$, da X^3+X+1 ein irreduzibles Polynom vom Grad 3 über $\mathbb{F}_2$ ist. Ausserdem ist $\mathbb{F}_8^\times$ zyklisch der Ordnung 7, also ist jedes von 1 verschiedene Element ein Erzeugendes. Zum Beispiel können wir das Bild von X in $\mathbb{F}_2[X]/(X^3+X+1)$ als erzeugendes Element wählen. Sein Minimalpolynom ist natürlich X^3+X+1.

   Sei $p^r = 9$. Dann ist $\mathbb{F}_9$ isomorph zu $\mathbb{F}_3[X]/(X^2+1)$, da X^2+1 ein irreduzibles Polynom vom Grad 2 über $\mathbb{F}_3$ ist. Eine $\mathbb{F}_3$-Basis von $\mathbb{F}_9$ ist also $\{1, a\}$ mit $a^2 = -1$. Da $\mathbb{F}_9^\times$ zyklisch der Ordnung 8 ist, suchen wir ein Element der Ordnung 8. Die Elemente der Ordnungen 1, 2 und 4 sind respektive 1, -1 und $\pm a$. Somit kann zum Beispiel $a+1$ nur noch die Ordnung 8 haben. (Wir können dies auch direkt nachrechnen vermittels $(a+1)^2 = 2a$ und $(a+1)^4 = (2a)^2 = -4 = -1 \neq 1$.) Wegen $(a+1)^2 + (a+1) - 1 = 0$ und $a+1 \notin \mathbb{F}_3$ ist X^2+X-1 das Minimalpolynom von $a+1$ über $\mathbb{F}_3$.

   Sei $p^r = 16$. Das Polynom X^4+X+1 ist irreduzibel vom Grad 4 über $\mathbb{F}_2$; also ist $\mathbb{F}_{16} = \mathbb{F}_2(a)$ für ein Element a mit Minimalpolynom X^4+X+1 über $\mathbb{F}_2$. Da $\mathbb{F}_{16}^\times$ zyklisch der Ordnung $16-1 = 3\cdot 5$ ist, ist schon a selbst ein Erzeuger, sofern nicht $a^3 = 1$ oder $a^5 = 1$ ist. In diesem Fall wäre a eine Nullstelle von X^3-1 oder $X^5-1 = (X-1)(X^4+X^3+X^2+X+1)$, wohingegen aus Gradgründen jedes dieser Polynome teilerfremd zum irreduziblen Polynom X^4+X+1 ist. Dies kann also nicht sein, und a ist ein Erzeuger von $\mathbb{F}_{16}^\times$ mit dem Minimalpolynom X^4+X+1.

2. (a) Zeige, dass das Polynom $f(X) = X^3+3X+3$ irreduzibel in $\mathbb{F}_5[X]$ ist.
   (b) Sei α eine Nullstelle von f in einem algebraischen Abschluss von $\mathbb{F}_5$ und $\mathbb{F}_{125} = \mathbb{F}_5(\alpha)$. Berechne die Darstellungsmatrix des Frobeniusautomorphismus $\mathrm{Frob}_5 \colon \mathbb{F}_{125} \to \mathbb{F}_{125}$ in der Basis $(1, \alpha, \alpha^2)$.
   (c) Schreibe das Element $\beta := 1/(1-\alpha) \in \mathbb{F}_{125}$ als $\mathbb{F}_5$-Linearkombination von $1, \alpha$ und α^2.
   (d) Zeige, dass α die zyklische Gruppe $\mathbb{F}_{125}^\times$ erzeugt.

   Lösung: We denote elements of $\mathbb{F}_5$ just with integer numbers, so that $5 = 0$.

   (a) Since the polynomial $f \in \mathbb{F}_5[X]$ has degree 3, every proper decomposition of f has a linear factor, which means that f is irreducible if and only if it has no root

in $\mathbb{F}_5$. Since $f(0) = 3$, $f(1) = 2$, $f(2) = 2$, $f(3) = 4$ and $f(4) = 4$, we obtain that f has no root in $\mathbb{F}_5$, therefore it is irreducible in $\mathbb{F}_5$.

(b) Since α is a root of f, we have

$$\alpha^3 = -3\alpha - 3 = 2(\alpha + 1) \text{ and}$$
$$(\alpha + 1)^3 = \alpha^3 + 3\alpha^2 + 3\alpha + 1 = 3(\alpha^2 + 1),$$

which implies in particular that

$$\alpha^9 = -\alpha^2 - 1.$$

To compute the matrix of $\mathrm{Frob}_5 : x \mapsto x^5$ with respect to the basis $(1, \alpha, \alpha^2)$, where α is a root of f, we write down the images of 1, α and α^2 as $\mathbb{F}_5$-linear combinations of 1, α and α^2. We get the following:

$$\begin{aligned}
\mathrm{Frob}_5(1) &= 1 \\
\mathrm{Frob}_5(\alpha) &= \alpha^5 = \alpha^2 \cdot 2 \cdot (\alpha + 1) = 2\alpha^3 + 2\alpha^2 = -1 - \alpha + 2\alpha^2 \\
\mathrm{Frob}_5(\alpha^2) &= \alpha \cdot \alpha^9 = -\alpha^3 - \alpha = -2 + 2\alpha
\end{aligned}$$

Then the matrix associated to Frob_5 with respect to the basis $(1, \alpha, \alpha^2)$ is

$$M_{\mathrm{Frob}_5} = \begin{pmatrix} 1 & -1 & -2 \\ 0 & -1 & 2 \\ 0 & 2 & 0 \end{pmatrix}.$$

(c) Suppose that $\beta = \lambda + \mu\alpha + \nu\alpha^2$ for $\lambda, \mu, \nu \in \mathbb{F}_5$. Then the condition $1 = \beta(1 - \alpha)$ gives

$$1 = \lambda + (\mu - \lambda)\alpha + (\nu - \mu)\alpha^2 - \nu\alpha^3 = \lambda + 3\nu + (3\nu + \mu - \lambda)\alpha + (\nu - \mu)\alpha^2,$$

which is equivalent to

$$\begin{cases} \lambda + 3\nu = 1 \\ 3\nu + \mu - \lambda = 0 \\ \nu - \mu = 0. \end{cases}$$

Solving the equations backwards we obtain $\mu = \nu$, $\lambda = 4\nu$ and $7\nu = 1$, so that the unique solution is $(\lambda, \mu, \nu) = (2, 3, 3)$, and $\beta = 2 + 3\alpha + 3\alpha^2$.

(d) The group $\mathbb{F}_{125}^\times$ is cyclic of order $124 = 4 \cdot 31$, and by Lagrange's theorem applied to the subgroup $\langle\alpha\rangle$ we see that the order of α is a divisor of 124. We want to prove that indeed $\mathrm{ord}_{\mathbb{F}_{125}^\times}(\alpha) = 124$, and this can be done by checking that α^4 and α^{62} both differ from 1, since every proper divisor of 124 divides either 4 or 62. Of course, $\alpha^4 = 2(\alpha^2 + \alpha) \neq 1$, so that we are left to check that $\alpha^{62} \neq 1$. We have

$$\alpha^{62} = \alpha^{-1}(\alpha^9)^7 = -\alpha^{-1}(\alpha^2 + 1)^7.$$

To proceed with the computation, notice that

$$(\alpha^2+1)^3 = \alpha^6 + 3\alpha^4 + 3\alpha^2 + 1 = 4(\alpha+1)^2 + \alpha^2 + \alpha + 3\alpha^2 + 1 = 3\alpha^2 - \alpha,$$
$$(\alpha^2+1)^6 = (3\alpha^2-\alpha)^2 = -\alpha^4 - \alpha^3 + \alpha^2 = -\alpha^2 + \alpha - 2 \text{ and}$$
$$(\alpha^2+1)^7 = (-\alpha^2+\alpha-2)(\alpha^2+1) = -\alpha^4 - \alpha^2 + \alpha^3 + \alpha - 2\alpha^2 - 2 = \alpha.$$

Then

$$\alpha^{62} = -\alpha^{-1}\alpha = -1 \neq 1,$$

and we can conclude that α generates $\mathbb{F}_{125}^\times$.

3. Sei K ein Körper der Charakteristik $p > 0$ und sei $a \in K$.

   (a) Zeige, dass das Polynom $f(X) := X^p - X - a \in K[X]$ separabel ist.

   (b) Sei α eine Nullstelle von f in einem algebraisch abgeschlossenen Oberkörper L von K. Zeige die Mengengleichheit

   $$\{\beta \in L : f(\beta) = 0\} = \{\alpha + x : x \in \mathbb{F}_p\}.$$

   (c) Zeige, dass im Fall $a \notin \{y^p - y : y \in K\}$ die Körpererweiterung $K(\alpha)/K$ den Grad p hat. Was geschieht im Fall $a \in \{y^p - y : y \in K\}$?

   (d) Zeige, dass im Fall $a \notin \{y^p - y : y \in K\}$ die Gruppe $\mathrm{Aut}_K(K(\alpha))$ zyklisch der Ordnung p ist.

   (e) Konstruiere auf diese Weise für $K = \mathbb{F}_p$ einen Körper der Ordnung p^p.

Lösung: (a) We proved in the lecture that f is separable if and only if f and f' are coprime. Because $f'(X) = pX^{p-1} - 1 = -1$ this is indeed the case.

(b) Because f is separable and has degree p, it has exactly p roots in L. Therefore, both sets have the same finite cardinality, namely p, and to show that they are the same it suffices to show that one is included in the other. Recall that the Frobenius of degree p is a field endomorphism of L which is the identity on $\mathbb{F}_p$. Thus for all $x \in \mathbb{F}_p$ we have

$$f(\alpha + x) = (\alpha + x)^p - (\alpha + x) - a = \alpha^p + x^p - \alpha - x - a = f(\alpha) + x^p - x = 0.$$

Hence $\{\beta \in L : f(\beta) = 0\} \supset \{\alpha + x : x \in \mathbb{F}_p\}$ and the equality follows.

(c) We start with the easy case: If $a = y^p - y$ for some $y \in K$, then $\alpha = y \in K$ is a root of $f(X) = X^p - X - (y^p - y)$. By (b), any root of f is in K. This means that $K(\alpha) = K$ and f decomposes into linear factors over K.

Now assume that $a \notin \{y^p - y : y \in K\}$, i.e. $\forall y \in K\colon y^p - y \neq a$. Then all the roots $\alpha + x$ of f lie outside K, and we claim that f is irreducible. This claim then

implies that f ist the minimal polynomial of α over K so that $K(\alpha)$ has degree p over K.

To prove our claim, consider any monic factor $g \in K[X]$ of f. Then by (b) we have

$$g(X) = \prod_{x \in I} (X - \alpha - x)$$

in $L[X]$ for some nonempty subset $I \subseteq \mathbb{F}_p$. Set $d := |I| = \deg(g)$, which by construction satisfies $0 < d \leqslant p$. Then the coefficient of X^{d-1} in g is

$$-\sum_{x \in I} (\alpha + x) = -d\alpha - \sum_{x \in I} x.$$

This coefficient needs to be in K, and since $\sum_{x \in I} x \in \mathbb{F}_p \subseteq K$, this implies $d\alpha \in K$. As $\alpha \notin K$, this is only possible if $p|d$, which implies $d = p$. Thus any factor of f has degree $p = \deg(f)$ and is therefore equal to f. This makes f irreducible.

(d) Nach (c) ist $K(\alpha)$ ein Stammkörper des irreduziblen Polynoms f über K. Nach §5.7 der Zusammenfassung stehen folglich die Endomorphismen $\varphi\colon K(\alpha) \to K(\alpha)$ über K in Bijektion zu den Wurzeln von f in $K(\alpha)$. Wegen $[K(\alpha)/K] < \infty$ ist ausserdem jeder solche Endomorphismus bereits ein Automorphismus. Die Gruppe $\mathrm{Aut}_K(K(\alpha))$ steht also in Bijektion zu $\mathbb{F}_p$ und hat deshalb die Ordnung p. Da p eine Primzahl ist, kann $\mathrm{Aut}_K(K(\alpha))$ dann nur zyklisch sein.

(Tatsächlich ist die Bijektion zwischen $\mathrm{Aut}_K(K(\alpha))$ und $\mathbb{F}_p$ bereits ein Gruppenisomorphismus. Denn zu jedem $x \in \mathbb{F}_p$ sei φ_x der eindeutige Endomorphismus mit $\varphi_x(\alpha) = \alpha + x$. Für alle $x, y \in \mathbb{F}_p$ gilt dann

$$\varphi_x(\varphi_y(\alpha)) = \varphi_x(\alpha + y) = \varphi_x(\alpha) + \varphi_x(y) = (\alpha + x) + y = \alpha + (x + y) = \varphi_{x+y}(\alpha).$$

Die Eindeutigkeit der Bijektion zeigt dann $\varphi_x \circ \varphi_y = \varphi_{x+y}$; somit ist die Bijektion ein Homomorphismus und folglich ein Isomorphismus.)

(e) Nach (c) genügt es, das Element a in der Menge $\mathbb{F}_p \smallsetminus \{y^p - y : y \in \mathbb{F}_p\}$ zu wählen. Diese Menge ist gleich $\mathbb{F}_p \smallsetminus \{0\}$; also tut es zum Beispiel $a = 1$. Somit ist $X^p - X - 1 \in \mathbb{F}_p[X]$ irreduzibel, und jeder Stammkörper davon ist eine Erweiterung von $\mathbb{F}_p$ vom Grad p, also ein Körper der Ordnung p^p.

**4. Ein Ring, der alle Körperaxiome ausser vielleicht die Kommutativität der Multiplikation erfüllt, heisst eine *Divisionsalgebra* oder ein *Schiefkörper*. Der *Satz von Wedderburn* besagt, dass jeder endliche Schiefkörper kommutativ ist.

Wähle $n \geqslant 1$. Versuche für n Stunden, selbst einen Beweis dafür zu finden. Vergleiche das Resultat mit bekannten Beweisen, wie zum Beispiel hier:
`https://en.wikipedia.org/wiki/Wedderburn%27s_little_theorem`

*5. Sei p eine ungerade Primzahl. Für jede zu p teilerfremde ganze Zahl x ist das *Legendresymbol* $\left(\frac{x}{p}\right)$ definiert durch:

$$\left(\frac{x}{p}\right) := \begin{cases} 1 & \text{falls } \exists\, a \in \mathbb{Z}\colon x \equiv a^2 \text{ modulo } (p), \\ -1 & \text{sonst,} \end{cases}$$

was nur von der Restklasse von x modulo (p) abhängt. Das *quadratische Reziprozitätsgesetz* von Gauss besagt

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

für je zwei verschiedene ungerade Primzahlen p und q. Dies sei im Folgenden vorausgesetzt.

(a) Zeige

$$\left(\frac{x}{p}\right) \equiv x^{\frac{p-1}{2}} \text{ modulo } (p),$$

und dass diese Kongruenz das Legendresymbol eindeutig bestimmt.

(b) Zeige, dass für alle zu p teilerfremden ganzen Zahlen x und y gilt

$$\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right) \cdot \left(\frac{y}{p}\right).$$

(c) Beweise den *ersten Ergänzungssatz* zum quadratischen Reziprozitätsgesetz:

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

(d) Beweise den *zweiten Ergänzungssatz* zum quadratischen Reziprozitätsgesetz:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

[*Hinweis:* Setze $s := \frac{p-1}{2}$ und zeige $s! \equiv 2^s s!(-1)^{\frac{s(s+1)}{2}}$ modulo (p), unter Benutzung von $s! = (-1)^{\frac{s(s+1)}{2}} \prod_{j=1}^{s}(-1)^j j$ und $-j \equiv p - j$ modulo (p).]

(e) Finde Kongruenzbedingungen für p, die zu $\left(\frac{13}{p}\right) = 1$ äquivalent sind.

(f) Folgere, dass für eine Primzahl $p \equiv 6$ mod (13) nur endlich viele $n \in \mathbb{Z}^{>0}$ existieren, so dass $n! + n^p - n + 13$ ein Quadrat in $\mathbb{Z}$ ist.

(**g) Zeige, dass für alle p und x der Wert von $\left(\frac{x}{p}\right)$ in $O(\max\{\log|x|, \log p\})$ Schritten effektiv berechnet werden kann, falls ganze Zahlen y in $O(\log|y|)$ Schritten faktorisiert werden können.

Lösung: (a) Betrachte die beiden Homomorphismen

$$\begin{aligned} s\colon &\quad \mathbb{F}_p^\times \to \mathbb{F}_p^\times \quad a \mapsto a^2, \\ t\colon &\quad \mathbb{F}_p^\times \to \mathbb{F}_p^\times \quad a \mapsto a^{\frac{p-1}{2}}. \end{aligned}$$

Da p ungerade ist, hat $\mathrm{Kern}(s) = \{\pm 1\}$ die Ordnung 2. Nach Lagrange und dem Homomorphiesatz hat $\mathrm{Bild}(s)$ folglich die Ordnung $\frac{p-1}{2}$ und somit den Index 2. Sodann gilt für alle $a \in \mathbb{F}_p^\times$ die Gleichung $t(s(a)) = a^{p-1} = 1$; also haben wir $\mathrm{Bild}(s) \subset \mathrm{Kern}(t)$. Schliesslich ist t nicht der triviale Homomorphismus, da die Gleichung $t(a) = a^{\frac{p-1}{2}} = 1$ nur höchstens $\frac{p-1}{2} < |\mathbb{F}_p^\times|$ verschiedene Lösungen haben kann. Darum ist $\mathrm{Kern}(t)$ eine echte Untergruppe von $\mathbb{F}_p^\times$. Da sie aber die Untergruppe $\mathrm{Bild}(s)$ vom Index 2 enthält, muss $\mathrm{Kern}(t) = \mathrm{Bild}(s)$ sein.

Nach Konstruktion besteht $\mathrm{Bild}(s)$ aus allen Quadraten in $\mathbb{F}_p^\times$. Also ist $a \in \mathbb{F}_p^\times$ ein Quadrat genau dann, wenn $t(a) = a^{\frac{p-1}{2}} = 1$ ist. Wegen $(a^{\frac{p-1}{2}})^2 = a^{p-1} = 1$ gilt im anderen Fall $a^{\frac{p-1}{2}} = -1$. Wenn wir dies auf eine zu p teilerfremde ganze Zahl x übertragen, folgt, dass x kongruent zu einem Quadrat modulo p ist genau dann, wenn $x^{\frac{p-1}{2}} \equiv 1$ modulo (p) ist, und andernfalls ist $x^{\frac{p-1}{2}} \equiv -1$ modulo (p). Nach der Definition von $\left(\frac{x}{p}\right)$ ist dies genau die Kongruenz in (a).

[*Aliter:* Benutze, dass $\mathbb{F}_p^\times$ zyklisch ist, und übertrage die Rechnung auf $\mathbb{Z}/(p-1)\mathbb{Z}$.]

Wegen $p > 2$ ist $1 \not\equiv -1$ modulo (p); folglich ist das Legendresymbol durch diese Kongruenz schon eindeutig bestimmt. Damit ist (a) gezeigt.

(b) Aus (a) folgt

$$\left(\frac{xy}{p}\right) \equiv (xy)^{\frac{p-1}{2}} = x^{\frac{p-1}{2}} \cdot y^{\frac{p-1}{2}} \equiv \left(\frac{x}{p}\right) \cdot \left(\frac{y}{p}\right) \quad \text{modulo } (p).$$

Da die äusseren Werte in $\{\pm 1\}$ liegen, folgt wegen $p > 2$ schon die Gleichheit.

(c) folgt ebenfalls mit $x = -1$ direkt aus (a) und $p > 2$.

(d) Zuerst rechnen wir

$$s! \;=\; \prod_{j=1}^{s} j \;=\; \prod_{j=1}^{s} (-1)^j \prod_{j=1}^{s} (-1)^j j \;=\; (-1)^{\sum_{j=1}^{s} j} \prod_{j=1}^{s} j \;=\; (-1)^{\frac{s(s+1)}{2}} \prod_{j=1}^{s} (-1)^j j.$$

Dann teilen wir das letzte Produkt auf nach der Parität von j:

$$\prod_{j=1}^{s} (-1)^j j \;=\; \prod_{k=1}^{\lfloor \frac{s}{2} \rfloor} (2k) \prod_{k=1}^{\lceil \frac{s}{2} \rceil} (-(2k-1)) \;\equiv\; \prod_{k=1}^{\lfloor \frac{s}{2} \rfloor} (2k) \prod_{k=1}^{\lceil \frac{s}{2} \rceil} (p-2k+1) \quad \text{modulo } (p).$$

In der letzten Formel durchlaufen die Faktoren beider Produkte alle positiven geraden Zahlen $< p$ genau einmal. Also gilt

$$\prod_{j=1}^{s} (-1)^j j \;\equiv\; \prod_{\ell=1}^{s} (2\ell) \;=\; 2^s s! \quad \text{modulo } (p).$$

Insgesamt folgt damit

$$s! \;\equiv\; (-1)^{\frac{s(s+1)}{2}} 2^s s! \quad \text{modulo } (p).$$

Wegen $0 < s = \frac{p-1}{2} < p$ ist aber $p \nmid s!$; durch Kürzen erhalten wir also

$$2^{\frac{p-1}{2}} \;=\; 2^s \;\equiv\; (-1)^{\frac{s(s+1)}{2}} \;=\; (-1)^{\frac{p^2-1}{8}} \quad \text{modulo } (p).$$

Mit (a) folgt nun

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

(e) Für jede Primzahl $p \neq 13$ besagt das quadratische Reziprozitätsgesetz

$$\left(\frac{13}{p}\right) = \left(\frac{p}{13}\right) \cdot (-1)^{\frac{p-1}{2}\frac{13-1}{2}} = \left(\frac{p}{13}\right).$$

Wir müssen also nur die Quadrate in $\mathbb{F}_{13}^{\times}$ bestimmen. In $\mathbb{F}_{13}$ haben wir

$$(\pm 1)^2 = 1,\ (\pm 2)^2 = 4,\ (\pm 3)^2 = -4,\ (\pm 4)^2 = 3,\ (\pm 5)^2 = -1,\ (\pm 6)^2 = -3.$$

Also ist $\left(\frac{13}{p}\right) = 1$ genau dann, wenn $p \equiv \pm 1$, ± 3 oder ± 4 modulo 13 ist.

(f) Schreibe $\gamma_p(n) := n! + n^p - n + 13$. Für jedes $n \geqslant p$ gilt $p | n!$; ausserdem ist $n^p \equiv n \bmod (p)$ nach dem kleinen Satz von Fermat. Also ist dann $\gamma_p(n) \equiv 13 \bmod (p)$. Ist nun $\gamma_p(n)$ ein Quadrat in $\mathbb{Z}$, so ist folglich 13 kongruent zu einem Quadrat modulo (p). Nach der Voraussetzung $p \equiv 6 \bmod (13)$ und (e) ist aber $\left(\frac{13}{p}\right) = -1$, und wir erhalten einen Widerspruch. Somit ist $\gamma_p(n)$ für kein $n \geqslant p$ ein Quadrat in $\mathbb{Z}$. Insbesondere gibt es nur endlich viele (nämlich weniger als p) positive ganze Zahlen n, für die $\gamma_p(n)$ ein Quadrat ist.

(g) Hinweis: Vergleiche die Situation mit der für den euklidischen Algorithmus.