Endliche Körper

Skript zur Vorlesung im SS 2000

19. Juli 2000

Inhaltsverzeichnis

1 Grundlegende Konstruktionen **5**

1.1 Der Polynomring 5

1.2 Automorphismen 14

1.3 Einheitswurzeln und Kreisteilungspolynome 21

1.4 Norm und Spur 27

2 Grundlegende Algorithmen **33**

2.1 Faktorisierung von Polynomen 33

3 Normalbasen **43**

Kapitel 1

Grundlegende Konstruktionen

1.1 Der Polynomring

Im 1. Kapitel folgen wir zunächst dem hervorragenden Text von J. Cigler [1]. Im übrigen erinnern wir uns an die Einführung in die Theoretische Informatik, Teil II. Das Übungsblatt »Ringe, Ideale und Restklassenringe, $\mathbb{Z}/k\mathbb{Z}$, Polynomringe« beinhaltet insbesondere den:

1.1. Satz:
Der Restklassenring $\mathbb{Z}/p\mathbb{Z}$ ist genau dann ein Körper, wenn p eine Primzahl ist.

Beweis. Ist p Primzahl und $0 < a < p$, so ist a zu p teilerfremd, d.h. $\mathrm{ggT}(a, p) = 1$. Es existieren also $k, l \in \mathbb{Z}$ mit $ka + lp = 1$ (BÉZOUT-Relation, erweiterter euklidischer Algorithmus). Liest man dies mod p, so gilt: $ka \equiv 1 \mod p$. Die Restklasse $a + (p)$ hat also $k + (p)$ als Inverse. Insgesamt: Jedes Element $\neq 0$ in $\mathbb{Z}/p\mathbb{Z}$ ist invertierbar, d.h. $\mathbb{Z}/p\mathbb{Z}$ ist ein Körper. Ist p eine zusammengesetzte Zahl, so existieren in $\mathbb{Z}/p\mathbb{Z}$ Nullteiler, so daß insbesondere kein Körper vorliegt. □

Bemerkung:
Dieser Beweis ist konstruktiv, da ein Algorithmus zur Inversion von Elementen angegeben wird. Überdies ist der Euklidische Algorithmus von fundamentaler Bedeutung. Beachte, daß Part I in [3] den Titel „EUCLID“ trägt.

1.2. Definition:
$\mathbb{F}_p$ bezeichnet den Körper mit p Elementen.

Ein erstes Ziel wird sein, alle endlichen Körper kennenzulernen. Wir werden sehen, daß es für jede Primpotenz im wesentlichen genau einen Körper dieser Größe gibt. Der Weg dahin führt notwendig über den *Polynomring* $\mathbb{F}_p[X]$.

1.3. Definition:
Ist R ein kommutativer Ring mit Eins, und $R \ni p \neq 0$ keine Einheit, so heißt dieses Element *unzerlegbar*, falls in jeder Darstellung $p = ab$, $a, b \in R$, ein Faktor eine Einheit ist. Die unzerlegbaren Elemente im Polynomring $R[X]$ heißen *irreduzible Polynome*.

Analog zu Satz (1.1) haben wir den

1.4. Satz:
Der Restklassenring $k[X]/(p)$ des Polynomrings über einem Körper ist genau dann ein Körper, wenn $p(X)$ ein irreduzibles Polynom ist.

Beweis. Es sei $p(X)$ irreduzibel vom Grad d: $\deg(p) = d$. Ist $0 \neq f(X) \in k[X]$ ein Polynom vom Grad $< d$, so gilt $\mathrm{ggT}(f(X), p(X)) = 1$. Der größte gemeinsame Teiler ist darstellbar als

$$1 = a(X)f(X) + b(X)p(X)$$

mit Polynomen $a(X), b(X) \in k[X]$, d.h.

$$1 \equiv a(X)f(X) \mod p(X)$$

Die Restklasse $f(X) + (p(X))$ hat $a(X) + (p(X))$ als Inverse. Zur Umkehrung genügt, wie in Satz (1.1), der Hinweis auf Nullteiler. □

1.5. Beispiele:
Wir geben als Anwendung von (1.4) Körper mit 4 und 8 Elementen.

1. In $\mathbb{F}_2[X]$ ist X^2+X+1 irreduzibel, da es keine Nullstellen in $\mathbb{F}_2$ hat. Es gibt 4 Polynome in $\mathbb{F}_2$ mit Grad < 2: $0, 1, X, X+1$. Die Beziehung $1 \equiv X(X+1)$ mod $(X^2 + X + 1)$ besagt, daß die Restklassen $\overline{X}$ und $\overline{1+X}$ zueinander invers sind. Die Multiplikationstafel ist:

$\times$	1	X	$1+X$
1	1	X	$1+X$
X	X	$1+X$	1
$1+X$	$1+X$	1	X

   Beachte, daß mod 2 gilt: $(1 + X)^2 \equiv 1 + X^2 \equiv X \mod (X^2 + X + 1)$. Es wird also „doppelt modular“ gerechnet: mod 2 und mod $(X^2 + X + 1)$.

2. In $\mathbb{F}_2[X]$ ist $X^3 + X + 1$ irreduzibel, da keine Nullstellen in $\mathbb{F}_2$ vorhanden sind.

   N.B. Die Tatsache „$p(X)$ hat im Grundkörper keine Nullstellen“ ist ab Grad 4 nicht mehr hinreichend für die Irreduzibilität!

Es gibt 8 Polynome in $\mathbb{F}_2$ vom Grad < 3: $0, 1, X, X+1, X^2, X^2+1, X^2+X, X^2+X+1$. Man gebe die Multiplikationstafel an. Man findet u.a.

$$\begin{aligned} X(X^2+1) &\equiv 1 \mod (X^3+X+1) \\ (X+1)(X^2+X) &\equiv 1 \mod (X^3+X+1) \\ X^2(X^2+X+1) &\equiv 1 \mod (X^3+X+1) \end{aligned}$$ ◀

1.6. Beobachtung:
Wie die Beispiele zeigen, ist der Ausgangskörper (hier $\mathbb{F}_2$) Teil des neuen, größeren Körpers. Das ist allgemein so: die Abbildung

$$\begin{cases} k \to k[X] \\ c \mapsto c \qquad \text{(konstantes Polynom)} \end{cases}$$

ist ein injektiver Homomorphismus in den Polynomring, die sog. *Konstanteneinbettung*: $k \hookrightarrow k[X]$. Bildet man weiter den Restklassenring $K := k[X]/p(X)$, $p(X)$ irreduzibel, so enthält der Körper K eine isomorphe Kopie von k in der Menge der Restklassen mod $p(X)$ der konstanten Polynome.

1.7. Definition:
Sind zwei Körper K, k ineinander enthalten: $K \supseteq k$, so spricht man von einer *Körpererweiterung*, oft auch mit $K \mid k$ notiert.

So ist beispielsweise $\mathbb{C}$ eine Körpererweiterung von $\mathbb{R}$:

$$\mathbb{R} \hookrightarrow \mathbb{R}[X]/(X^2+1) \cong \mathbb{C}$$

Die Konstruktion in (1.4) hat die bemerkenswerte Konsequenz, die auf LEOPOLD KRONECKER (1823-1891) zurückgeht:

1.8. Existenz von Wurzeln im Erweiterungskörper:
Ist $f(X) \in k[X]$ ein Polynom vom Grad > 1, dann existiert ein Erweiterungskörper $K \supseteq k$, in dem $f(X)$ eine Nullstelle besitzt.

Zur **Illustration** führen wir dies am Beispiel (1.5) 2. vor: $p(X) = X^3+X+1 \in \mathbb{F}_2[X]$ ist in $\mathbb{F}_2$ ohne Nullstelle. In dem konstruierten Körper mit 8 Elementen $K_8 := \mathbb{F}_2[X]/(X^3+X+1)$ hat $p(X)$ eine Nullstelle. Man nehme $\alpha := X \bmod p(X)$, die Restklasse von X, und rechne nach:

$$p(\alpha) = \alpha^3 + \alpha + 1 = X^3 + X + 1 \equiv 0 \mod p(X)$$

Tatsächlich enthält $\mathbb{F}_8$ noch 2 weitere Nullstellen von $p(X)$: wir dividieren den linearen Faktor $X - \alpha$ aus X^3+X+1 ab (beachte: die Berechnung spielt sich in $K_8[X]$ ab!):

$$X^3 + X + 1 = (X - \alpha)(X^2 + \alpha X + \alpha^2 + 1)$$

Man beobachtet, daß α^2 Nullstelle von $X^2 + \alpha X + \alpha^2 + 1$ ist. Erneute Division ergibt

$$X^2 + \alpha X + \alpha^2 + 1 = (X - \alpha^2)(X + \alpha^2 + \alpha)$$

Beachte, daß $\alpha^4 = \alpha^2 + \alpha$. Also sind α, α^2 und α^4 die 3 Nullstellen von $p(X)$ in K_8. Wir werden in Kürze sehen, warum hier die fortlaufende Quadrierung auftritt.

Nun der

Beweis von (1.8). Hat k selbst eine Nullstelle von $f(X)$, so ist nichts zu zeigen. Ansonsten hat jeder irreduzible Faktor $p(X)$ von $f(X)$ einen Grad > 1. Dann ist $K := k[X]/(p(X))$ ein Körper, der k (via Konstanteneinbettung, s.o.) umfaßt. In K gilt $p(\overline{X}) = 0$, genauer: $p(X \bmod p(X)) = 0$, d.h. $X \bmod p(X) \in K$ ist Nullstelle von $f(X)$. □

Möglicherweise zerfällt f nun in lauter lineare Faktoren über K. Wenn nicht, kann man das Verfahren mit über K irreduziblen Faktoren vom Grad > 1 wiederholen, so daß k nach endlich vielen Schritten in einen Körper eingebettet ist, in dem f komplett in Linearfaktoren zerfällt.
In der Algebra spricht man von dem *Zerfällungskörper* von f über $\mathbb{F}_p$.

Es soll nun gezeigt werden, daß mit dem *Konstruktionsprinzip* „$k[X]/\,(p(X))$“ alle endlichen Körper erfaßt werden. Zunächst muß geklärt werden, was es bedeutet, neben Polynomen in $\mathbb{F}_p[X]$ die zugehörige *Polynomfunktionen* zu betrachten. Wir betrachten die Abbildung

$$\varphi : \begin{cases} \mathbb{F}_p[X] \to \mathcal{F}_p \\ f(X) \mapsto \tilde{f} \end{cases}$$

wobei $\mathcal{F}_p$ die Menge der Funktionen ${\mathbb{F}_p}^{\mathbb{F}_p}$ und $\tilde{f}$ die zu f gehörige Polynomfunktion bezeichnet. Man beachte, daß jede Funktion $f : \mathbb{F}_p \to \mathbb{F}_p$ eine Polynomfunktion ist: wegen der Endlichkeit stimmt f mit dem LAGRANGEschen Interpolationspolynom vom Grad $p - 1$ überein! *. Dieser Sachverhalt wird auch so benannt: die endlichen Körper sind *funktional vollständig*. Der obige Homomorphismus ist also surjektiv. Da $\mathcal{F}_p$ endlich ist, ist der Kern von φ von endlichem Index. Genauer: $\ker \varphi = (X^p - X)$, das vom Polynom $X^p - X$ in $\mathbb{F}_p[X]$ erzeugte Ideal. Dies ist eine Konsequenz des bekannten Satzes:

1.9. Kleiner Satz von FERMAT:
Für alle $a \in \mathbb{F}_p$ gilt: $a^p \equiv a \bmod p$.

*Der kleine Satz von FERMAT liefert: ist $f : \mathbb{F}_p \to \mathbb{F}_p$ eine Funktion, so leistet das Polynom $F(X) = \sum_{\gamma \in \mathbb{F}_p} f(\gamma)(1 - (X - \gamma)^{p-1})$ tatsächlich das Gewünschte: $f(\alpha) = F(\alpha) \quad (\forall \alpha \in \mathbb{F}_p)$.

Beweis. Nach dem Satz von LAGRANGE ist für endliche Gruppen die Ordnung einer Untergruppe $U \sqsubseteq G$ stets ein Teiler der Gruppenordnung von G. Betrachten wir nun ein Element a aus der multiplikativen Gruppe ${\mathbb{F}_p}^\times$. Dann gilt innerhalb dieser Gruppe $|\langle a\rangle| \mid p-1$. Daher ist $a^{p-1} = 1$ und $a^p = a$. □

Mit anderen Worten: $X^p - X$ hat in $\mathbb{F}_p$ genau p Nullstellen:

$$X^p - X = \prod_{a \in \mathbb{F}_p} (X - a)$$

Die zugehörige Polynomfunktion ist identisch Null: $\widetilde{X^p - X} = 0$ auf $\mathbb{F}_p$. Also ist $X^p - X$ Element von $\ker \varphi$. Ist umgekehrt $f \in \ker \varphi$, so verschwindet f an allen Stellen $a \in \mathbb{F}_p$, d.h. $\prod_{a\in\mathbb{F}_p}(X-a)$ ist ein Teiler von f. Damit ist $\ker \varphi = (X^p - X)$ bewiesen.

Insgesamt haben wir gezeigt:

1.10. Satz:
Der Ring $\mathbb{F}_p[X]/(X^p - X)$ ist isomorph zum Funktionenring $\mathcal{F}_p$.

Auf jedem kommutativen Ring R mit Eins wirkt der Ring $\mathbb{Z}$ auf *kanonische* Weise:

$$\rho : \begin{cases} \mathbb{Z} \to R \\ n \mapsto n \cdot 1 = \underbrace{1 + 1 + \cdots + 1}_{n \text{ mal}} \end{cases}$$

ρ ist homomorph, also $\operatorname{im}\rho = \mathbb{Z}/(p)$, $p \geq 0$, da $\mathbb{Z}$ Hauptidealring ist.

1.11. Definition:
Die eindeutig bestimmte Zahl $p \geq 0$ heißt *Charakteristik* des Rings. Ist R ein Körper k, so ist p eine Primzahl: $\operatorname{char}(k) = p$ oder 0. Ist k Körper, so heißt der von 1 erzeugte Körper der *Primkörper* von k.

Bemerkung:
Der Primkörper ist isomorph zu $\mathbb{Q}$, falls k die Charakteristik Null hat. Ist die Charakteristik gleich p, so ist $\mathbb{F}_p$ der Primkörper.

1.12. Satz:
Ist k ein endlicher Körper von Charakteristik p, so ist $|k| = p^n$, wobei $n = \dim_{\mathbb{F}_p}(k)$.

Beweis. Betrachte k als Vektorraum über dem Primkörper $\mathbb{F}_p$. □

Tatsächlich werden wir jetzt sehen, daß es für jede Primzahl p und jeden Exponenten n einen Körper mit p^n Elementen gibt. Überdies ist dieser bis auf Isomorphie eindeutig bestimmt. Von fundamentaler Bedeutung ist folgende Tatsache:

1.13. Satz:
Die multiplikative Gruppe $k^\times = k\backslash\{0\}$ jedes *endlichen* Körpers ist zyklisch.

Zum Beweis brauchen wir zwei Hilfsaussagen. Die erste werden wir noch häufig benötigen.

1.14. Lemma:
Ist k ein Körper, so hat ein Polynom $f \in k[X]$ vom Grad n höchstens n Nullstellen in k.

Beweis. Ist $\alpha \in k$ irgendeine Stelle, so existiert ein *eindeutig* bestimmtes Polynom $g \in k[X]$ mit

$$f(X) - f(\alpha) = (X - \alpha)g(X) \qquad (*)$$

Ist nämlich $f = \sum_{i=0}^{n} a_i X^i$, so ist $f(X) - f(\alpha) = \sum_{i=1}^{n} a_i(X^i - \alpha^i)$ und $\forall i \geq 1$ gilt $X - \alpha \mid X^i - \alpha^i$. Also: $X - \alpha \mid f(X) - f(\alpha)$. Definiere g als Quotienten. Andererseits folgt aus $0 = (X-\alpha)[g(X)-h(X)]$ notwendig $g \equiv h$. Ist α Nullstelle von f, so ergibt $(*)$, daß $X - \alpha$ ein Teiler von $f(X)$ ist. Jeder Nullstelle von f entspricht also ein linearer Faktor in der Zerlegung von f in irreduzible Faktoren. Aufgrund der Nullteilerfreiheit von k folgt die Behauptung. □

Man beachte, daß in Ringen mit Nullteilern die Aussage (1.14) falsch ist. Z.B. sind alle Elemente von $\mathbb{Z}/(6)$ Nullstellen von $X^3 - X$.

1.15. Lemma:
Es sei G ein endliche, abelsche Gruppe. Hat die Gleichung $x^d = 1$ für jeden Teiler $d \mid |G|$ höchstens d Lösungen in G, so ist G zyklisch.

Beweis. (C.F. GAUSS) Sei $|G| = n$ und $g \in G$ ein Element von Ordnung d. Beachte: $d \mid n$ nach dem Satz von LAGRANGE. Die Elemente $1, g, g^2, \ldots, g^{d-1}$ sind genau d Lösungen von $x^d = 1$. Nach Voraussetzung sind das somit alle Lösungen der Gleichung! Daher gibt es in G entweder 0 oder $\varphi(d)$ Elemente der Ordung d. Sei $\#(d)$ diese Anzahl:

$$n = |G| = \sum_{d|n} \#(d) \leq \sum_{d|n} \varphi(d) = n$$

Das ist nur möglich, wenn für alle $d \mid n$ gilt $\#(d) = \varphi(d)$, also auch für den größten Teiler: $\#(n) = \varphi(n) > 0$. Es gibt also mindestens ein Element der Ordnung n. Also: G ist zyklisch. □

1.16. Definition:
Ist k ein endlicher Körper, so heißt jedes Element von $k^\times$, welches diese zyklische Gruppe erzeugt, ein *primitives Element* von k.

Beispiele:

a) In $\mathbb{F}_7$ ist 3 primitiv: $1 = 3^0, 3 = 3^1, 2 = 3^2, 6 = 3^3, 4 = 3^4, 5 = 3^5$. Dagegen ist 2 in $\mathbb{F}_7$ nicht primitiv. Wegen $\varphi(6) = 2$ sind 3 und 5 die beiden primitiven Elemente von $\mathbb{F}_7$.

b) Ist k ein endlicher Körper von Ordnung q, und ist $q-1$ eine Primzahl, so ist jedes Element in $k^\times$ primitiv. Beispiele sind $\mathbb{F}_2, \mathbb{F}_3$ und die bereits konstruierten Körper der Ordnungen 4 und 8. Zur Erinnerung: eine Primzahl der Gestalt $2^n - 1$ heißt MERSENNEsche Primzahl; der Exponent n ist notwendig auch prim.◀

N.B. Es gibt kein deterministisches Verfahren zur Konstruktion von primitiven Elementen in k. In $\mathbb{F}_p$ geht man der Reihe nach die quadratfreien Reste $2 \le i < p$ durch und testet ihre Ordnung. Die Erfahrung zeigt, daß das kleinste primitive Element nach $\log p$ Schritten auftaucht.

Wir sind nun in der Lage, Existenz und Eindeutigkeit endlicher Körper herzuleiten.

1.17. Satz:
Jeder endliche Körper k der Charakteristik p ist isomorph zu einem Restklassenkörper von $\mathbb{F}_p[X]$ modulo einem irreduziblen Polynom $f(X)$:

$$k \cong \mathbb{F}_p[X]/\left(f(X)\right)$$

Es gibt also genau einen Körper mit p^n Elementen, wenn es ein *irreduzibles* Polynom $f(X) \in \mathbb{F}_p[X]$ vom Grad n gibt.

Beweis. Da k nach (1.13) ein primitives Element α besitzt und $|k| = q = p^n$, siehe (1.12), sind $0, \alpha, \alpha^2, \ldots, \alpha^{q-1} = 1$ die Elemente von k. Die Abbildung

$$\mathrm{eval}_\alpha : \begin{cases} \mathbb{F}_p[X] \to k \\ \sum a_i X^i \mapsto \sum a_i \alpha^i \end{cases}$$

ist also ein surjektiver Ringhomomorphismus auf k, der sog. *Auswertungshomomorphismus.* Jedes Polynom wird hier bei α ausgewertet. $\ker \mathrm{eval}_\alpha$ ist ein Hauptideal, etwa $\ker \mathrm{eval}_\alpha = (f(X))$, wobei f das eindeutig bestimmte normierte Polynom kleinsten Grades in $\ker \mathrm{eval}_\alpha$ ist. Wir haben also: $k \cong \mathbb{F}_p[X]/(f(X))$. Wäre $f(x)$ reduzibel, so hätte dieser Restklassenring Nullteiler. Hat f den Grad n, so hat der Restklassenring die Größe p^n. □

Um einen Körper der vorgelegten Größe p^n zu konstruieren, brauchen wir ein irreduzibles Polynom vom Grad n über $\mathbb{F}_p$. Diese Aufgabe wird später im Mittelpunkt des Interesses stehen. Im Augenblick wählen wir folgenden Ausweg:

1.18. Verallgemeinerung des kleinen Satzes von FERMAT:
Ist k ein endlicher Körper mit $|k| = p^n$ Elementen, so genügt jedes der p^n Elemente der Gleichung

$$X^{p^n} - X = 0$$

Beweis. $|k^\times| = p^n - 1$. Also gilt für jedes $\alpha \in k^\times$: $\alpha^{p^n-1} = 1$ oder so: $\alpha^{p^n} = \alpha$. Da auch 0 letzterer Beziehung genügt, folgt (1.18). □

Dieses Polynom wird nun zur Erzeugung von einem Körper mit p^n Elementen benutzt:

1.19. Satz:
Ist k ein Körper mit $|k| = p^n$ Elementen, so ist k gleich der Nullstellenmenge von $X^{p^n} - X \in \mathbb{F}_p[X]$.

Beweis. Sei $q := p^n$. Zunächst einmal zeigt folgende Überlegung, daß $X^q - X$ keine mehrfachen Nullstellen hat (wo immer diese sein mögen): Ist α Nullstelle von $X^q - X$, d.h. $\alpha^q - \alpha = 0$, so gilt

$$X^q - X = X^q - \alpha^q - X + \alpha = (X-\alpha)^q - (X-\alpha) = (X-\alpha)[(X-\alpha)^{q-1} - 1]$$

was zeigt, daß der Linearfaktor $(X-\alpha)$ nur einfach vorkommt.† Ferner sieht man, daß die Nullstellen von $X^q - X$ tatsächlich einen Körper bilden: Gilt $\alpha^q = \alpha$ und $\beta^q = \beta$, so auch $(\alpha/\beta)^q = \alpha/\beta$. Ferner gilt wegen Charakteristik p: $(\alpha \pm \beta)^p = \alpha^p \pm \beta^p$, was durch n-malige Anwendung zu $(\alpha \pm \beta)^{p^n} = \alpha^{p^n} \pm \beta^{p^n}$ führt. □

Bemerkung:
In der Algebra spricht man (1.19) so aus: „der" Körper mit p^n Elementen ist „der" Zerfällungskörper von $X^{p^n} - X$ über $\mathbb{F}_p$. Während wir über die Eindeutigkeit des Zerfällungskörpers nichts sagen wollen, können wir jedoch beweisen:

1.20. Theorem (Existenz und Eindeutigkeit endlicher Körper):
Für jede Primzahlpotenz $q = p^n$ gibt es bis auf Isomorphie genau einen Körper mit q Elementen, das sogenannte GALOIS-Feld $\mathbb{F}_q$, auch mit $\mathrm{GF}(p)$ bezeichnet. Es fällt mit dem Zerfällungskörper von $X^q - X \in \mathbb{F}_p[X]$ zusammen. Insbesondere gibt es für jedes prime p und jedes $n \geq 1$ stets ein Polynom vom Grad n, das über $\mathbb{F}_p$ irreduzibel ist.

Beweis. Wir haben den Satz (1.19) bereits bewiesen und zeigen nun, daß zwei Körper $\mathbb{K}$ und $\mathbb{L}$ gleicher Mächtigkeit p^n isomorph sind. Es sei $\alpha \in \mathbb{K}$ ein primitives Element. Aus dem Beweis von (1.17) sieht man, daß es ein irreduzibles Polynom f über $\mathbb{F}_p$ gibt mit α als Nullstelle (der dort fixierte Erzeuger von

†I.N. HERSTEIN: *Math. Monthly*, March 1987, p.290

ker eval(α)). Wir betrachten $d := \mathrm{ggT}(f(X), X^{p^n} - X)$. Da α eine gemeinsame Nullstelle von f und $X^{p^n} - X$ ist, ist α auch Nullstelle von d, d.h. $d \in \ker \mathrm{eval}(\alpha)$. Also $f \mid d$. Das ergibt wegen der Normiertheit: $f = d$, mit anderen Worten $f \mid X^{p^n} - X$. Nach (1.19): $X^{p^n} - X$ zerfällt über $\mathbb{L}$ in lauter lineare Faktoren, d.h. es gibt ein $\beta \in \mathbb{L}$ mit $f(\beta) = 0$. Nun ist die Zuordnung $\sum_{i=0}^{n-1} c_i \alpha^i \mapsto \sum_{i=0}^{n-1} c_i \beta^i$ ein gewünschter Isomorphismus zwischen $\mathbb{K}$ und $\mathbb{L}$. □

1.21. Korollar:
Sei k ein Körper mit p^n Elementen und seien f und g irreduzible Polynome über $\mathbb{F}_p$, beide vom Grad n. Dann existiert ein Isomorphismus $\mathbb{F}_p[X]/(f) \cong \mathbb{F}_p[X]/(g)$.

Wir betrachten die Verhältnisse genauer in $\mathbb{F}_9$ und in $\mathbb{F}_{16}$.

Beispiele:

1. $\mathbb{F}_9$

   Sowohl $f = X^2 + X + 2$ als auch $g = X^2 + 1$ sind irreduzibel über $\mathbb{F}_3$. In $\mathbb{F}_9$ hat f die Nullstelle $\alpha := X \bmod f$. Die Elemente von $\mathbb{F}_9$ sind also in dieser Darstellung:

   $$\{0, 1, 2, \alpha, \alpha + 1, \alpha + 2, 2\alpha, 2\alpha + 1, 2\alpha + 2\}$$

   Ebenso hat g in $\mathbb{F}_9$ die Nullstelle $i := X \bmod g$ und $\mathbb{F}_9$ ist entsprechend

   $$\{0, 1, 2, i, i + 1, i + 2, 2i, 2i + 1, 2i + 2\}$$

   Die „Umrechnung“ geschieht so:

   $0 = \alpha^2 + \alpha + 2 = (\alpha + 2)^2 + 1$, d.h. $\alpha + 2 = \pm i$.

   Wir dürfen annehmen[‡], daß die Wurzeln α und i so gewählt sind, daß $\alpha + 2 = i$ gilt. Die Abbildung $\sum_{k=0}^{1} c_k \alpha^k \mapsto \sum_{k=0}^{1} c_k (1 + i)^k$ ist dann die identische Abbildung auf $\mathbb{F}_9$. Sie induziert einen Isomorphismus von $\mathbb{F}_3[X]/(f)$ auf $\mathbb{F}_3[X]/(g)$. Dem Beweis von (1.20) entnehmen wir, daß f und g Teiler von $X^9 - X$ sind. Tatsächlich lautet die vollständige Faktorisierung:

   $$\begin{aligned} X^9 - X =& X(X - 1)(X + 1)(X - i)(X + i)(X - i + 1) \\ & (X + i + 1)(X + i - 1)(X - i - 1) \\ =& X(X^2 - 1)(X^2 + 1)(X^2 + 2X + 2)(X^2 + X + 2) \end{aligned}$$

[‡] In der Tat: hätten wir die Beziehung $\alpha + 2 = -i$, so würden wir die Wurzel i durch die andere Wurzel $-i$ ersetzen.

Das Element α ist primitiv, während wegen $i^4 = 1$ i nicht primitiv ist. Die Potenzen von α sind:

$$\begin{aligned}
\alpha^1 &= \alpha = 1 + i \\
\alpha^2 &= 2\alpha + 1 = -i \\
\alpha^3 &= (1+i)^3 = 1 + i^3 = 1 - i \\
\alpha^4 &= (-i)^2 = -1 \\
\alpha^5 &= \alpha^4 \cdot \alpha = -(1+i) = -1 - i \\
\alpha^6 &= (\alpha^2)^3 = -i^3 = i \\
\alpha^7 &= \alpha^6 \cdot \alpha = -1 + i \\
\alpha^8 &= (\alpha^4)^2 = 1
\end{aligned}$$

2. $\mathbb{F}_{16}$

Man kann zeigen (vgl. später), daß die folgenden 3 Polynome die einzigen über $\mathbb{F}_2$ irreduziblen Polynome vom Grad 4 sind

$$\begin{aligned}
f &= X^4 + X + 1 \\
f^* &= X^4 + X^3 + 1 \\
g &= X^4 + X^3 + X^2 + X + 1
\end{aligned}$$

Die kanonischen Nullstellen von f und f^* sind jeweils primitiv in $\mathbb{F}_{16}$. Wegen $g = (X^5 - 1)/(X - 1)$ erfüllen die Wurzeln ω von g die Beziehung $\omega^5 = 1$, sind also nicht primitiv. ◀

1.2 Automorphismen

Es ist wichtig, die Ringendomorphismen $\varphi : \mathbb{F}_q \to \mathbb{F}_q$ zu kennen. Diese sind injektiv, da $\mathbb{F}_q$ ein Körper ist, und somit bijektiv, da $\mathbb{F}_q$ endlich ist.

1.22. Definition:
Die Abbildung $\sigma_p : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ mit $\sigma_p(\alpha) = \alpha^p$, $\alpha \in \mathbb{F}_{p^n}$ wird als FROBENIUS-Automorphismus bezeichnet.

Wie wir wissen, ist $\alpha \mapsto \alpha^p$ homomorph, also nach obigen Bemerkungen automorph. Entscheidend für alle folgenden Anwendungen ist

1.23. Satz:
Ist $f \in \mathbb{F}_p[X]$ und $\alpha \in \mathbb{F}_{p^n}$ Nullstelle von f, so ist $\sigma_p(\alpha) = \alpha^p$ ebenfalls Nullstelle von f.

Beweis. Den kleinen Satz von FERMAT (1.9) kann man jetzt so aussprechen:

$$\forall a \in \mathbb{F}_p : \sigma_p(a) = a$$

Infolgedessen gilt für das Polynom $f = \sum a_i X^i$ mit $f(\alpha) = 0$:

$$f(\alpha^p) = \sum a_i (\alpha^p)^i = \sum a_i^p (\alpha^i)^p = \left(\sum a_i \alpha^i\right)^p = f(\alpha)^p = 0$$

□

1.24. Satz:
Ist $f \in \mathbb{F}_p[X]$ irreduzibel vom Grad n und ist α eine Nullstelle von f in einem Körper $K \supset \mathbb{F}_p$, so sind die $\sigma_p^i(\alpha) = \alpha^{p^i}$ $(0 \le i \le n-1)$ **alle** Nullstellen von f:

$$f(x) = (X - \alpha)(X - \alpha^p) \cdots (X - \alpha^{p^{n-1}}) \in K[X]$$

Diese sind paarweise verschieden und heißen die *Konjugierten* von α.

Beweis. Wegen (1.23) bleibt zu zeigen, daß die α^{p^i} paarweise verschieden sind. Aus $\alpha^{p^i} = \alpha^{p^j}$ $0 \le i < j \le n-1$ erhalten wir durch i-fache Anwendung des inversen Automorphismus σ_p^{-1} die Gleichung $\alpha = \alpha^{p^{j-i}}$. Setze $k := j - i$. Wir bilden nun das Hilfspolynom

$$g(X) = (X - \alpha)(X - \alpha^p) \cdots (X - \alpha^{p^{k-1}})$$

und berechnen $\sigma_p(g(X))$. Dabei benutzen wir, daß sich $\sigma_p \in \mathrm{Aut}(\mathbb{F}_{p^n})$ auf dem Polynomring fortsetzt via

$$\sigma_p\left(\sum a_i X^i\right) = \sum \sigma_p(a_i) X^i = \sum a_i^p X^i$$

Ergebnis:

$$\sigma_p(g) = (X - \alpha^p)(X - \alpha^{p^2}) \cdots (X - \alpha^{p^{k-1}})(X - \alpha)$$

d.h. die Faktoren werden nur vertauscht und somit gilt $\sigma_p(g) = g$. Also werden alle Koeffizienten von g von σ_p fixiert, liegen also im Grundkörper $\mathbb{F}_p$: $g(x) \in \mathbb{F}_p[X]$. Wegen $f(\alpha) = g(\alpha) = 0$ und f irreduzibel müßte g ein Vielfaches von f sein, was der Gradbedingung $k < n$ widerspricht. □

1.25. Satz:
Die Gruppe der Automorphismen von $\mathbb{F}_{p^n}$ ist zyklisch von Ordnung n und wird vom FROBENIUS-Automorphismus σ_p erzeugt.

Beweis. Wie im Beweis zu (1.17) betrachten wir ein primitives Element α von $\mathbb{F}_{p^n}$ und das zugehörige normierte Polynom $f \in \mathbb{F}_p[X]$ kleinsten Grades mit $f(\alpha) = 0$. Ist φ ein Automorphismus von $\mathbb{F}_{p^n}$, so gilt $\varphi(1) = 1$ und $\varphi(2) = \varphi(1+1) = \varphi(1) + \varphi(1) = 2$ usw., d.h. $\varphi|_{\mathbb{F}_p} = \mathrm{id}\,|_{\mathbb{F}_p}$: der Primkörper wird elementweise fixiert. Die Fortsetzung von φ auf den Polynomring fixiert demnach auch f: $\varphi(f) = f$. Ferner gilt $f(\varphi(\alpha)) = \varphi(f(\alpha)) = \varphi(0) = 0$, so daß auch $\varphi(\alpha)$ Nullstelle von f ist. Nach (1.24) gilt: $\varphi(\alpha) = \alpha^{p^k}$ für ein k. $\varphi(\alpha) = \sigma_p^k(\alpha)$. Dies gilt auch für alle Potenzen von α: $\varphi(\alpha^i) = \varphi(\alpha)^i = (\sigma_p^k(\alpha))^i = \sigma_p^k(\alpha^i)$. Also stimmt φ mit σ_p^k überein. □

1.26. Definition:
Ist $\alpha \in \mathbb{F}_{p^n}$, so bezeichnen wir das normierte Polynom kleinsten Grades $\in \mathbb{F}_p[X]$ mit α als Nullstelle als das *Minimalpolynom von α über $\mathbb{F}_p$*.

Bemerkung:
Die letztere Relativierung „über $\mathbb{F}_p$" weist darauf hin, daß man das Minimalpolynom auch bezüglich Zwischenkörpern betrachten kann. Die Struktur der Zwischenkörper ist nun gefragt:

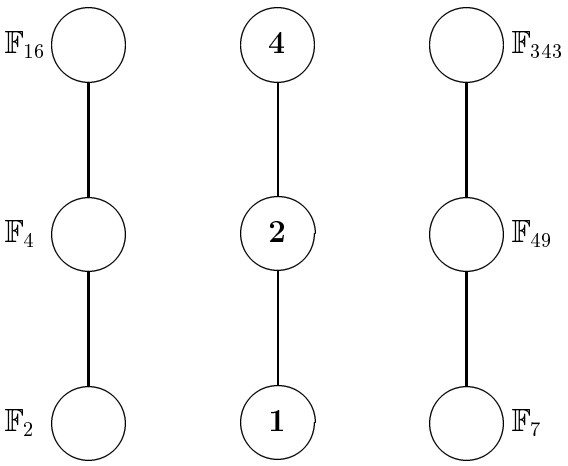
1.27. Satz:
$\mathbb{F}_{p^n}$ hat genau dann einen zu $\mathbb{F}_{p^s}$ isomorphen Teilkörper, wenn $s \mid n$ gilt. Dieser ist dann eindeutig bestimmt und besteht aus allen Wurzeln in $\mathbb{F}_{p^n}$ der Gleichung $X^{p^s} - X = 0$.

Beweis. Ist F_{p^s} ein Teilkörper, so besteht er aus den p^s Nullstellen des Polynoms $X^{p^s} - X$. Gäbe es einen zweiten Teilkörper gleicher Ordnung, so widerspräche dies Lemma (1.14). Ist $\mathbb{F}_{p^s} \subset \mathbb{F}_{p^n}$, so ist $\mathbb{F}_{p^n}$ ein Vektorraum über $\mathbb{F}_{p^s}$, d.h. $p^n = (p^s)^k = p^{sk}$, also $s \mid n$.

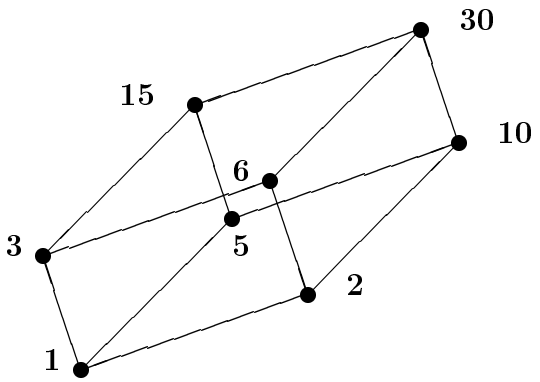
Ist $s \mid n$ gegeben, etwa $sk = n$, so folgt $p^s - 1 \mid p^n - 1$ (geometrische Reihe) und ebenso $X^{p^s-1} - 1 \mid X^{p^n-1} - 1$ und schließlich $X^{p^s} - X \mid X^{p^n} - X$. Die Elemente α in $\mathbb{F}_{p^n}$ mit $\alpha^{p^s} = \alpha$ bilden einen Teilkörper, nämlich $\mathbb{F}_{p^s}$, in $\mathbb{F}_{p^n}$. □

Beispiel:
Nach (1.27) gibt es in $\mathbb{F}_{16}$ genau einen Teilkörper $\mathbb{F}_4$. Wir präsentieren $\mathbb{F}_{16}$ in der Form $\mathbb{F}_{16} = \mathbb{F}_2[X]/(X^4 + X + 1)$. Die kanonische Nullstelle $\alpha := X \bmod (X^4 + X + 1)$ ist primitiv, d.h. hat Ordnung 15. Die Lösungen der Gleichung $X^4 - X = 0$ sind demnach $\{0, 1, \alpha^5, \alpha^{10}\}$. Denn hat α Ordnung 15, so hat α^5 Ordnung 3. α^5 ist Wurzel des Polynoms $X^2 + X + 1 \in \mathbb{F}_2[X]$. Die Konjugierte von α^5 ist $\sigma_2(\alpha^5) = \alpha^{10}$. Beachte: $(X + \alpha^5)(X + \alpha^{10}) = X^2 + (\alpha^5 + \alpha^{10})X + \alpha^{15} = X^2 + X + 1$. ◀

Bemerkung:
Der Verband der Teilkörper von $\mathbb{F}_{p^n}$ entspricht also dem Verband der Teiler von n (und ist demnach unabhängig von p (!)).



oder komplizierter: $n = 30$



Die zentrale Rolle des Polynoms $X^{p^n} - X \in \mathbb{F}_p[X]$ ist durch die bisherigen Überlegungen deutlich geworden. Der Beweis zu Theorem (1.20) zeigt auch, daß für jedes Element in $\mathbb{F}_{p^n}$ das zugehörige Minimalpolynom Teiler von $X^{p^n} - X$ ist. Es gilt genauer:

1.28. Satz:
Das Polynom $X^{p^n} - X \in \mathbb{F}_p[X]$ ist das Produkt aller irreduziblen Polynome über $\mathbb{F}_p$, deren Grade Teiler von n sind.

Beweis. Sei $f \in \mathbb{F}_p[X]$ irreduzibel vom Grad d, wobei $d \mid n$ sei. Dann ist $f \mid X^{p^d} - X$ (siehe Beweis zu (1.20)). In (1.27) wurde benutzt: $p^d - 1 \mid p^n - 1$. Also auch $X^{p^d} - X \mid X^{p^n} - X$. Ist umgekehrt $f(X) \mid X^n - X$ vom Grad d, so erzeugen die Nullstellen von f einen Teilkörper von $\mathbb{F}_{p^n}$ (vgl. (1.19)) mit p^d Elementen. Nach (1.27) gilt: $d \mid n$. □

1.29. Beispiele:
Die kleinsten Beipiele in $\mathbb{F}_2[X]$ kommen immer wieder vor:

$$\begin{aligned}
X^2 - X &= X(X+1) \\
X^4 - X &= X(X+1)(X^2+X+1) \\
X^8 - X &= X(X+1)(X^3+X+1)(X^3+X^2+1) \\
X^{16} - X &= X(X+1)(X^2+X+1)(X^4+X+1) \\
&\quad (X^4+X^3+1)(X^4+X^3+X^2+X+1) \blacktriangleleft
\end{aligned}$$

Für größere p und n werden diese Zerlegungen sehr kompliziert. Oft braucht man jedoch nur eine Übersicht über die auftretenden Grade der Faktoren. Dazu formulieren wir (1.24) erneut:

Ist ω ein primitives Element in $\mathbb{F}_{p^n}$ und $\alpha = \omega^i$ $(0 \leq i \leq p^n - 2)$ ein Element von ${\mathbb{F}_{p^n}}^\times$, so hat das Minimalpolynom von α die Gestalt

$$m_i(X) = (X - \omega^i)(X - \omega^{ip}) \cdots (X - \omega^{ip^{d-1}}) \qquad (*)$$

wobei $d \mid n$. Der Teiler $d = d(i)$ kennzeichnet den kleinsten Teilkörper $\mathbb{F}_{p^n}$, in dem ω^i liegt.

1.30. Definition:
Die Menge der in $(*)$ auftretenden Exponenten

$$C_i := \{i, ip, \ldots, ip^{d-1}\}$$

heißt eine *Kreisteilungsklasse* (cyclotomic coset) von p modulo $p^n - 1$. Dabei ist d die kleinste Zahl ≥ 0 mit $ip^d \equiv i \mod (p^n - 1)$.

Im Beispiel $\mathbb{F}_{16}$ sehen die Kreisteilungsklassen so aus:

$$\begin{aligned}
C_1 &= \{1, 2, 4, 8\} \\
C_3 &= \{3, 6, 12, 9\} \\
C_5 &= \{5, 10\} \\
C_7 &= \{7, 14, 13, 11\} \\
C_0 &= \{0\}
\end{aligned}$$

Wie ersichtlich, bezeichnen wir mit C_j die Klasse, in der j der minimale Repräsentant ist. Diese einfache Berechnung zeigt: $X^{15} - 1$ zerfällt in ein irreduzibles Polynom vom Grad 1, ein irreduzibles Polynom vom Grad 2 und 3 irreduzible Polynome vom Grad 4. $\blacktriangleleft$

Bemerkung:
Wesentlich in Definition (1.30) ist, daß p zu $p^n - 1$ teilerfremd ist und somit die Abbildung $i \mapsto i \cdot p$ eine Permutation auf $\mathbb{Z}/(p^n - 1)$ darstellt. Man kann also auch Kreisteilungsklassen in jedem Kontext (q, N) mit $\mathrm{ggT}(q, N) = 1$ und $i \mapsto iq \mod N$ betrachten.

Beispiel:
$q = 2$, $N = 9$. Die Zerlgung $C_0 = \{0\}$, $C_1 = \{1, 2, 4, 8, 7, 5\}$, $C_3 = \{3, 6\}$ „sagt voraus“, daß $X^9 - 1$ über $\mathbb{F}_2$ in 3 irreduzible Faktoren von Graden $1, 2, 6$ zerfällt. Tatsächlich gilt:

$$\begin{aligned} X^9 - 1 &= (X^3)^3 - 1 \\ &= (X^3 - 1)(X^6 + X^3 + 1) \\ &= (X - 1)(X^2 + X + 1)(X^6 + X^3 + 1) \end{aligned}$$ ◀

N.B.:
Dies ist ein Beweis für die Irreduzibilität von $X^6 + X^3 + 1$ über $\mathbb{F}_2$!

Der Spezialfall $n = 1$ von (1.28) ist wieder der kleine Satz von FERMAT (1.9):

1.31. Korollar:
In $\mathbb{F}_p[X]$ gilt

$$X^p - X = X(X - 1)(X - 2) \cdots (X - (p - 1))$$

Speziell ergibt sich durch Koeffizientenvergleich bei X der **Satz von** WILSON:

$$(p - 1)! \equiv -1 \mod p$$

Vergleicht man in (1.28) die Grade, so ergibt sich der

1.32. Satz:
Bezeichnet $N_p(d)$ die Anzahl der irreduziblen Polynome vom Grad d, über $\mathbb{F}_p$, so gilt

$$p^n = \sum_{d|n} d \cdot N_p(d)$$

□

Für kleine n kann man diese implizite Formel für die Zahlen $N_p(d)$ auch auswerten: Ist $p = 2$ und $n = 6$, so folgt aus $2^6 = N_2(1) + 2N_2(2) + 3N_2(3) + 6N_2(6)$ und $N_2(1) = 2$, $N_2(2) = 1$, $N_2(3) = 2$ die Information: $N_2(6) = 9$. Diese 9 Polynome explizit zu bestimmen, ist eine kompliziertere Aufgabe. ◀

In der elementaren Zahlentheorie zeigt man, wie Beziehungen der Art (1.32) mittels sogenannter MÖBIUS-*Inversion* umgekehrt werden können. Das führt zum Resultat

1.33. Theorem:

$$N_p(n) = \frac{1}{n} \sum_{d|n} \mu(\frac{n}{d}) p^d$$

wobei μ die MÖBIUS-Funktion bezeichnet:

$$\mu(m) = \begin{cases} 1 & \text{für } m = 1 \\ (-1)^s & \text{falls } m \text{ quadratfrei mit } s \text{ Primfaktoren} \\ 0 & \text{falls } m \text{ nicht quadratfrei} \end{cases}$$

Der Beweis von (1.33) würde den Gang der Dinge unnötig unterbrechen, wir wollen aber (1.33) an zwei Beispielen erläutern:

$$\begin{aligned} N_2(6) &= \frac{1}{6}[\mu(6)2^1 + \mu(3)2^2 + \mu(2)2^3 + \mu(1)2^6] \\ &= \frac{1}{6}(2 - 4 - 8 + 64) = 9 \end{aligned}$$

$$\begin{aligned} N_2(12) &= \frac{1}{12}[\mu(12)2^1 + \mu(6)2^2 + \mu(4)2^3 + \mu(3)2^4 + \mu(2)2^6 + \mu(1)2^{12}] \\ &= \frac{1}{12}(4 - 16 - 64 + 4096) = 335 \end{aligned}$$

Das Wachstum der Zahlen $N_p(n)$ kann wie folgt abgeschätzt werden:

1.34. Korollar:
Für den Anteil $\frac{N_p(n)}{n}$ der irreduziblen normierten Polynome an allen normierten Polynomen vom Grad n gilt:

$$(1 - 2p^{-n/2})/n \leq \frac{N_p(n)}{p^n} \leq \frac{1}{n}(1 - \frac{1}{p^{n-1}})$$

Beweis. Die obere Schranke folgt aus (1.32), wenn man alle Teiler $1 < d < n$ vernachlässigt:

$$p^n \geq nN_p(n) + p$$

Zum Beweis der unteren Schranke benutzt man $\mu(k) \leq 1$ für alle $k \geq 1$:

$$|nN_p(n) - p^n| \leq \sum_{\substack{d|n \\ d \neq n}} p^d \leq \frac{p^{n/2+1}}{p-1} \leq 2p^{n/2}$$

□

Bemerkung:
Diese Abschätzung hat eine probabilistische Interpretation: wählt man ein normiertes Polynom vom Grad n in $\mathbb{F}_p[X]$ zufällig, so ist dies mit einer Wahrscheinlichkeit von etwa $1/n$ irreduzibel. Die Frage, wie man ein Polynom auf Irreduzibilität testet, wird in Kapitel 3 beantwortet.

1.3 Einheitswurzeln und Kreisteilungspolynome

N.B.:
Im folgenden gehen wir stets von einem Grundkörper $\mathbb{F}_q$ aus, der nicht notwendig Primkörper ist. Der Leser möge sich im Zweifelsfall davon überzeugen, daß dies zulässig ist.

Nach (1.28) ist $X^{q^n} - X$ das Produkt **aller** über $\mathbb{F}_q$ irreduziblen normierten Polynome von Graden, die n teilen. Wir werden dieses Produkt auf mehrere Weisen in „Schichten" einteilen. Zunächst sortieren wir nach den auftretenden Graden:

1.35. Definition:
$I(q, n; X)$ sei das Produkt aller normierten, über $\mathbb{F}_q$ irreduziblen Polynome vom Grad n. Somit gilt:

$$X^{q^n} - X = \prod_{d|n} I(q, d; X)$$

Mittels der multiplikativen Version der Möbius-Umkehrung (siehe Anhang) erhalten wir:

1.36. Satz:

$$\begin{aligned} I(q, n; X) &= \prod_{d|n} (X^{q^d} - X)^{\mu(\frac{n}{d})} \\ &= \prod_{d|n} (X^{q^{\frac{n}{d}}} - X)^{\mu(d)} \\ &\quad \text{falls } n > 1 \\ &= \prod_{d|n} (X^{q^d - 1} - 1)^{\mu(\frac{n}{d})} \end{aligned}$$

Beispiel:
$q = 2; n = 4$:

$$\begin{aligned} I(2, 4; X) &= (X^{16} - X)^{\mu(1)} (X^4 - X)^{\mu(2)} (X^2 - X)^{\mu(4)} \\ &= \frac{X^{16} - X}{X^4 - X} = \frac{X^{15} - 1}{X^3 - 1} \\ &= X^{12} + X^9 + X^6 + X^3 + 1 \end{aligned}$$

Man überzeugt sich, daß dieses Polynom tatsächlich gleich dem Produkt $(X^4 + X + 1)(X^4 + X^3 + 1)(X^4 + X^3 + X^2 + X + 1)$ ist. Wie wir wissen, haben die Wurzeln von $X^4 + X + 1$ und $X^4 + X^3 + 1$ die Ordnung 15, während $X^4 + X^3 + X^2 + X + 1$ Wurzeln von Ordnung 5 hat. ◄

Ziel ist nun, die Faktoren von $I(q,n;X)$ nach Ordnungen zu sortieren. Dazu müssen wir etwas ausholen und uns über die *Kreisteilungspolynome* informieren.

1.37. Definition:
Sei $n>0$. Der Zerfällungskörper von $X^n-1\in K[X]$ über K heißt *Kreisteilungskörper* (cyclotomic field) von X^n-1 über K, i.Z. $K^{@n}$. Die Wurzeln von X^n-1 in $K^{@n}$ heißen n-te Einheitswurzeln, i.Z. $E^{@n}$.

Die Theorie über $\mathbb{Q}$ ist sehr verwickelt. Über $K=\mathbb{F}_p$ ist es leichter:

1.38. Satz:
Sei $n>0$ und K ein Körper der Charakteristik p. Dann gilt:

1. Falls $p\nmid n$, so ist $E^{@n}$ bezüglich Multiplikation in $K^{@n}$ eine zyklische Gruppe der Ordnung n.
2. Sei $p\mid n$, etwa $n=p^em$ mit $\mathrm{ggT}(m,p)=1$. Dann ist $K^{@n}=K^{@m}$ und $E^{@n}=E^{@m}$. Die Wurzeln von X^n-1 in $K^{@n}$ sind die Elemente von $E^{@m}$, jeweils mit Vielfachheit p^e.

Beweis. 1. Sei $n\geq 2$: X^n-1 hat wegen $\mathrm{ggT}(p,n)=1$ nur einfache Nullstellen. Sind $\zeta,\nu\in E^{@n}$, so gilt $(\zeta\nu^{-1})^n=\zeta^n\nu^{-n}=1$, d.h. $E^{@n}$ ist eine *Gruppe*. Wie in Satz (1.13) wird $E^{@n}$ als *zyklisch* nachgewiesen.

2. Es gilt: $X^{p^em}-1\equiv(X^m-1)^{p^e}\mod p$.

□

1.39. Definition:
Sei K ein Körper mit Charakteristik $p>0$, ferner $n>0$ mit $p\nmid n$. Jeder Erzeuger der zyklischen Gruppe $E^{@n}$ heißt eine *primitive n-te Einheitswurzel* über K.

1.40. Definition:
Sei K ein Körper der Charakteristik $p>0$ und ζ eine primitive n-te Einheitswurzel über K.

$$Q_n(X)=\prod_{\substack{1\leq s\leq n\\ \mathrm{ggT}(s,n)=1}}(X-\zeta^s)$$

heißt das *n-te Kreisteilungspolynom* über K.

Beachte:
Für den Grad gilt: $\deg Q_n(X)=\varphi(n)$. Nach Definition ist $Q_n(X)\in K^{@n}[X]$. Man sieht jedoch, daß $Q_n(x)\in K[X]$ ist:

1.41. Satz:
Sei K ein Körper der Charakteristik p mit $p\nmid n$. Dann gilt:

1. $X^n - 1 = \prod_{d|n} Q_d(X)$.

2. Die Koeffizienten von $Q_n(X)$ liegen in $\mathbb{F}_q$, falls $\mathrm{char}(k) > 0$ ist, ansonsten liegen sie in $\mathbb{Z}$.

Beweis. 1. Sei ζ ein primitives Element in $E^{\textcircled{n}}$. Für eine Potenz ζ^s gilt:

$$\mathrm{ord}(\zeta^s) = \frac{n}{\mathrm{ggT}(n,s)} =: d$$

und ζ^s ist primitive d-te Einheitswurzel. In $X^n - 1 = \prod_{s=1}^{n}(X - \zeta^s)$ sind offenbar alle Elemente von Ordnung d in $Q_d(X)$ versammelt, und das für alle $d \mid n$.

2. Induktion über n. Beachte: $Q_n(X)$ ist *normiert*.

$n = 1$: $Q_1(X) = X - 1$ ✓ (Induktionsanker)

$n > 1$: Induktionsannahme: Sei die Behauptung wahr für alle $1 \leq d < n$. Wegen (1) gilt $Q_n(X) = (X^n - 1)/\prod_{\substack{d|n \\ d\neq n}} Q_d(X)$, wobei

$$Q_d[X] \in \begin{cases} \mathbb{F}_p[X] & \text{für } \mathrm{char}(K) > 0 \\ \mathbb{Z}[X] & \text{sonst.} \end{cases} \quad \text{(nach Induktionsannahme)}$$

Mit *langer Division* folgt die Behauptung.

□

Beispiele:

(a)

$$\begin{aligned} Q_{15} &= \frac{X^{15} - 1}{(X^4 + X^3 + X^2 + X + 1)(X^2 + X + 1)(X - 1)} \\ &= X^8 - X^7 + X^5 - X^4 + X^3 - X + 1 \end{aligned}$$

Wir wissen, daß dieses Polynom über $\mathbb{F}_2$ zerfällt:

$$Q_{15} \equiv (X^4 + X^3 + 1)(X^4 + X + 1) \mod 2$$

(b)

$$Q_p[X] = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + 1, \quad \text{falls } p \text{ eine Primzahl ist.}$$

(c) Sei p eine Primzahl. Dann gilt:

$$Q_{p^r}(X) = \frac{X^{p^r}-1}{Q_1(X)Q_p(X)\cdots Q_{p^{r-1}}(X)} = \frac{X^{p^r}-1}{X^{p^{r-1}}-1}$$
$$= \sum_{j=0}^{p-1} X^{j\cdot p^{r-1}} = Q_p(X^{p^{r-1}})$$

Zum Beispiel: $Q_4(X) = (X+1)_{X\leftarrow X^2} = X^2+1$

(d)

$$Q_{12} = \frac{X^{12}-1}{Q_6Q_4Q_3Q_2Q_1} = \frac{(X^{12}-1)Q_3Q_2Q_1}{(X^6-1)Q_4Q_3Q_2Q_1}$$
$$= \frac{X^6+1}{Q_4} = \frac{X^6+1}{X^2+1} = X^4-X^2+1 \quad \blacktriangleleft$$

1.42. Satz:
Sei K ein Körper.

(a) Falls $K=\mathbb{Q}$ ist, so gilt: Q_n ist irreduzibel über $\mathbb{Q}$.

(b) Ist $K=\mathbb{F}_q$ und $\mathrm{ggT}(q,n)=1$ (o.B.d.A.), so zerfällt Q_n in $\varphi(n)/d$ viele *normierte irreduzible* Faktoren gleichen Grades d über K. $K^{\textcircled{n}}$ ist der Zerfällungskörper jeder dieser Faktoren und $[K^{\textcircled{n}}:K]=d=\mathrm{ord}_n(q)$, d.h. d ist minimal mit $q^d\equiv 1 \mod n$.

Beweis. **(a)** wird in der Algebra bewiesen.

(b) Sei η eine primitive n-te Einheitswurzel über $\mathbb{F}_q$:

$$\eta\in\mathbb{F}_{q^k} \leftrightarrow \eta^{q^k}=\eta, \quad \text{d.h. } n \mid q^k-1$$

Sei d minimal mit $n\mid q^d-1$, d.h. $d=\mathrm{ord}_n(q)$: Das Minimalpolynom von η hat den Grad d.

□

Die bisher abgeleiteten Rechenregeln reichen nicht aus, um $Q_n(X)$ für große n effizient zu berechnen. Ein erster Schritt in diese Richtung ist die Beobachtung, daß (1.41) (1) mittels Möbius-Inversion umgeschrieben werden kann:

1.43. Satz:
Für jeden Körper K und jedes $n\in\mathbb{N}$ ist das n-te Kreisteilungspolynom $Q_n(X)$ gegeben durch

$$Q_n(X) = \prod_{d\mid n}(X^d-1)^{\mu(\frac{n}{d})} = \prod_{d\mid n}(X^{\frac{n}{d}}-1)^{\mu(d)}$$

In endlicher Charakteristik p muß dabei $p\nmid n$ gelten. □

Beispiel:

$$Q_{12} = \frac{(X^{12}-1)(X^2-1)}{(X^6-1)(X^4-1)} = \frac{X^6+1}{X^2+1} = X^4 - X^2 + 1 \quad \blacktriangleleft$$

Bemerkung:
Der Rechenaufwand bei den auftretenden Divisionen wird reduziert durch zwei Beobachtungen:

1. $\deg(Q_n) = \varphi(n)$. Man rechne also stets $\bmod X^{\varphi(n)}$.
2. Die Polynome Q_n sind selbstreziprok. Man rechne also $\bmod X^{\frac{\varphi(n)}{2}+1}$.

Wir verdeutlichen das Vorgehen am Beispiel Q_{30}.

Beispiel:

$$Q_{30} = \frac{(X^2-1)(X^3-1)(X^5-1)(X^{30}-1)}{(X-1)(X^6-1)(X^{10}-1)(X^{15}-1)}$$

$\varphi(30) = 8$ und $\varphi(30)/2 + 1 = 5$.
Ist $i \geq 5$, so gilt $(X^i-1)(X^i+1) \equiv -1 \mod X^5$. Also $(X^6-1)^{-1} \equiv (X^{10}-1)^{-1} \equiv (X^{15}-1)^{-1} \equiv -1 \mod X^5$ und ebenso $X^5 - 1 \equiv X^{30} - 1 \equiv -1 \mod X^5$. Es bleibt:

$$Q_{30}(X) \equiv \frac{X^2-1}{X-1}(X^3-1)(-1) \equiv -X^4 - X^3 + X + 1 \mod X^5$$

Ergebnis: $Q_{30} = X^8 + X^7 - X^5 - X^4 - X^3 + X + 1$. $\blacktriangleleft$

Nun zu einem wirklich effizienten Verfahren, das von H. LÜNEBURG in [7] §14 beschrieben wird.

1.44. Lemma:

$$Q_{mn}(X) \mid Q_n(X^m), \quad n, m \in \mathbb{N}$$

□

1.45. Lemma:
Sind $m, n \in \mathbb{N}$ derart, daß jeder Primteiler von m auch n teilt, so gilt:

$$Q_{mn}(X) = Q_n(X^m)$$

Beweis. Gradvergleich!

$$\varphi(mn) = mn \prod_{p \mid mn} (1 - \frac{1}{p}) = mn \prod_{p \mid n} (1 - \frac{1}{p}) = m\varphi(n)$$

□

1.46. Lemma:
Ist $n \in \mathbb{N}$, $p \nmid n$, p prim, so gilt:

$$Q_n(X) \cdot Q_{np}(X) = Q_n(X^p)$$

Beweis. Ist ζ primitive n-te Einheitswurzel, so auch ζ^p, da $\mathrm{ggT}(n,p) = 1$. Also ist außer $Q_{np}(X)$ (nach (1.44)) auch $Q_n(X)$ Teiler von $Q_n(X^p)$. Diese Polynome sind relativ prim, so daß auch deren Produkt $Q_n(X^p)$ teilt. Schließlich stimmt wieder der Grad. □

1.47. Algorithmus zur Berechnung von $Q_n(X)$:
Ist $n = \prod {p_i}^{e_i}$ vorgelegt, so bezeichne $\mathrm{soc}(n) = \prod p_i$ den quadratfreien Teil von n. Nach (1.45) gilt $Q_n(X) = Q_{\mathrm{soc}(n)}(X^{n/\mathrm{soc}(n)})$. Ist n gerade, so benutze bei der Berechnung von $Q_{\mathrm{soc}(n)}$ die Tatsache $Q_{2k}(X) = Q_k(-X)$ für ungerades k (vgl. Übungen). Die Basis $\mathrm{soc}(n) = p_1 \cdots p_s$ kann also als *ungerade* angenommen werden. Man verfährt nun rekursiv:

$$\begin{aligned} Q_{p_1}(X) &= \frac{X^{p_1}-1}{X-1} = \sum_{i=0}^{p_1-1} X^i \quad \text{Weiter nach (1.46).} \\ Q_{p_1p_2}(X) &= Q_{p_1}(X^{p_2})/Q_{p_1}(X) \\ Q_{p_1p_2p_3}(X) &= Q_{p_1p_2}(X^{p_3})/Q_{p_1p_2}(X) \quad \text{usf.} \end{aligned}$$

Ist $Q_{\mathrm{soc}(n)}$ berechnet, so substituiere schließlich $X \leftarrow X^{n/\mathrm{soc}(n)}$. □

Abschließend wollen wir noch die Polynome $I(q,n;X)$ in (1.35) weiter zerlegen:

1.48. Satz:
Für $n > 1$ gilt:

$$I(q,n;X) = \prod_m Q_m(X)$$

wobei m diejenigen Teiler von $q^n - 1$ durchläuft, für die gilt: $\mathrm{ord}_m(q) = n$.

Beweis. [§] Die multiplikative Version der Möbius-Inversion hat folgende Konsequenz:
die Gleichheit zweier Folgen $(s_n)_{n\geq 1} = (t_n)_{n\geq 1}$ ist gleichwertig mit der Gleichheit der multiplikatorischen Folgen

$$\left(\prod_{d|n} s_d\right)_{n\geq 1} = \left(\prod_{d|n} t_d\right)_{n\geq 1}$$

[§]Beweisidee: V. Strehl

Wir ergänzen die Behauptung noch um die triviale Beziehung für $n = 1$:

$$I(q,n;X) = \begin{cases} X \cdot \prod_{m|q-1} Q_m(X) & \text{für } n = 1 \\ \prod_{ord_m(q)=n} Q_m(X) & \text{für } n > 1 \end{cases}$$

Die linke Seite gefaltet ergibt nach (1.35)

$$\prod_{d|n} I(q,d;X) = X^{q^n} - X$$

und die rechte Seite faltet sich zu

$$X \prod_{d|n} \prod_{ord_m(q)=d} Q_m(X) = X \cdot \prod_{m|q^n-1} Q_m(X) = X(X^{q^n-1} - 1)$$

□

1.4 Norm und Spur

Für eine Körpererweiterung vom Grad n $\mathbb{F}_{q^n} \mid \mathbb{F}_q$ sind zwei Abbildungen von $\mathbb{F}_{q^n}$ nach $\mathbb{F}_q$ besonders wichtig:

1.49. Definition:
Die *Spur-Funktion* von $\mathbb{F}_{q^n} \mid \mathbb{F}_q$ ist

$$\mathrm{Tr}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = \sum_{i=0}^{n-1} \alpha^{q^i}$$

und die *Norm-Funktion* von $\mathbb{F}_{q^n} \mid \mathbb{F}_q$ ist

$$\mathrm{N}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = \prod_{i=0}^{n-1} \alpha^{q^i}$$

Der Kürze halber schreiben wir $\mathrm{Tr}_{q^n|q}$ und $\mathrm{N}_{q^n|q}$ oder, falls der Grundkörper fixiert ist, $\mathrm{Tr}_{n|1}$ und $\mathrm{N}_{n|1}$, bzw. nur Tr und N. Die Eigenschaften der Funktionen fassen wir zusammen in

1.50. Satz:
Es sei $\mathbb{F}_q \subset \mathbb{F}_{q^n}$ eine Körpererweiterung vom Grad n. Für alle $\alpha, \beta \in \mathbb{F}_{q^n}$ und $\lambda \in \mathbb{F}_q$ gilt:

(a)	$\mathrm{Tr}(\alpha) \in \mathbb{F}_q$	(a')	$\mathrm{N}(\alpha) \in \mathbb{F}_q$
(b)	$\mathrm{Tr}(\alpha+\beta) = \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta)$	(b')	$\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\,\mathrm{N}(\beta)$
(c)	$\mathrm{Tr}(\lambda\alpha) = \lambda\,\mathrm{Tr}(\alpha)$	(c')	$\mathrm{N}(\lambda\alpha) = \lambda^n\,\mathrm{N}(\alpha)$
(d)	$\mathrm{Tr}(\alpha^q) = \mathrm{Tr}(\alpha)$	(d')	$\mathrm{N}(\alpha^q) = \mathrm{N}(\alpha)$
(e)	Tr ist surjektiv auf F_q	(e')	N ist surjektiv auf $\mathbb{F}_q$

Beweis. Wir zeigen nur die Eigenschaften der Spur.

(a) $\mathrm{Tr}(\alpha) \in \mathbb{F}_q$ bedeutet $\mathrm{Tr}(\alpha)^q = \mathrm{Tr}(\alpha)$. Tatsächlich erfahren die Summanden in $\alpha + \alpha^q + \cdots + \alpha^{q^{n-1}}$ einen ring-shift.

(b) Klar, da σ_q Automorphismus.

(c) $(\lambda\alpha)^q = \lambda\alpha^q$, da $\lambda \in \mathbb{F}_q$.

(d) vergleiche (a)

(e) Tr ist nach (a), (b) und (c) eine Linearform von $\mathbb{F}_{q^n}$ nach $\mathbb{F}_q$. Sie ist nicht identisch Null, sonst hätte das „Spurpolynom“ $X + X^q + \cdots + X^{q^{n-1}}$ im Widerspruch zu (1.14) q^n Nullstellen. Also ist das Bild 1-dimensional und der Kern von Tr entsprechend $(n-1)$-dimensional. Jedes Element $\lambda \in \mathbb{F}_q$ hat q^{n-1} viele Urbilder unter Trace. ¶

□

Beispiel:
F_{16} sei realisiert durch $\mathbb{F}_2/(X^4+X^3+X^2+X+1)$, α erfülle $\alpha^4 = \alpha^3+\alpha^2+\alpha+1$. Jedes $\beta \in \mathbb{F}_{16}$ hat bezüglich der Basis $\alpha^0, \alpha^1, \alpha^2, \alpha^3$ die Darstellung $\beta = \sum_{i=0}^{3} b_i\alpha^i$, kurz $\beta = [b_3, b_2, b_1, b_0]$. Wegen der Linearität ist $\mathrm{Tr}_{4|1}(\beta) = \sum_{i=0}^{3} b_i \,\mathrm{Tr}_{4|1}(\alpha^i)$. Es reicht also, die Spuren von $\alpha^0, \alpha^1, \alpha^2, \alpha^3$ zu berechnen. Da $\mathrm{Tr}(1) = 1+1+1+1 = 0$ und $\mathrm{Tr}(\alpha) = \mathrm{Tr}(\alpha^2) = \mathrm{Tr}(\alpha^4)$ ist auch $\mathrm{Tr}(\alpha^3) = \mathrm{Tr}(\alpha)$. Da die Spur nicht identisch verschwindet, gilt $\mathrm{Tr}(\alpha) = 1$. Somit ergibt sich die Spur eines beliebigen Elements als

$$\mathrm{Tr}(\beta) = [b_3, b_2, b_1, b_0][1, 1, 1, 0] = b_3 + b_2 + b_1$$

Eine solche Formel für die Spur ist basisabhängig! Man berechne die Spur für die beiden anderen Präsentationen von $\mathbb{F}_{16}$, nämlich $\mathbb{F}_2[X]/(X^4+X+1)$ und $\mathbb{F}_2[X]/(X^4+X^3+1)$. ◀

1.51. Satz (Transitivität der Spur):
Sind $\mathbb{F} := \mathbb{F}_q$, $\mathbb{E} := \mathbb{F}_{q^m}$ und $\mathbb{K} := \mathbb{F}_{q^{mn}}$ drei Körper, so gilt für alle $\alpha \in \mathbb{K}$:

$$\mathrm{Tr}_{mn|1}(\alpha) = \mathrm{Tr}_{m|1}(\mathrm{Tr}_{mn|m}(\alpha))$$

¶Die Aussage in (e) kann man auf „Polynomebene“ auch so sehen:

$$X^{q^n} - X = \prod_{c \in \mathbb{F}_q} \left(\sum_{i=0}^{n-1} X^{q^i} - c \right)$$

Die paarweise teilerfremden Polynome $f_c(X) := \sum_{i=0}^{n-1} X^{q^i} - c$ sind nämlich Teiler von $X^{q^n} - X$, was aus $f_c^q - f_c = X^{q^n} - X$ folgt. Die Nullstellen von f_c sind die q^{n-1} Elemente mit Spur $= c$.

Beweis.

$$\begin{aligned}\mathrm{Tr}_{m|1}(\mathrm{Tr}_{mn|m}(\alpha)) &= \sum_{i=0}^{m-1} \left(\mathrm{Tr}_{mn|m}(\alpha)\right)^{q^i} \\ &= \sum_{i=0}^{m-1} \left(\sum_{j=0}^{n-1} \alpha^{(q^m)^j} \right)^{q^i} \\ &= \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \alpha^{q^{jm+i}} \\ &= \sum_{k=0}^{mn-1} \alpha^{q^k} = \mathrm{Tr}_{mn|1}(\alpha) \ ,\end{aligned}$$

weil jede Zahl $0 \le k \le mn-1$ eine eindeutige Darstellung der Form $k = jm + i$ mit $j < n$ und $i < m$ hat. □

In der Situation $\mathbb{F} := F_q \subset \mathbb{F}_{q^n} =: \mathbb{K}$ sei $\alpha \in \mathbb{K}$ ein Element mit Minimalpolynom vom Grad n: $X^n + c_1 X^{n-1} + \cdots + c_n, c_i \in \mathbb{F}$. Die Nullstellen dieses irreduziblen Polynoms sind demnach $\alpha, \alpha^q, \alpha^{q^2}, \ldots \alpha^{q^{n-1}}$ und der Koeffizientenvergleich in $X^n + c_1 X^{n-1} + \cdots + c_n = \prod_{i=0}^{n-1}(X - \alpha^{q^i})$ liefert $c_1 = -\sum_{i=0}^{n-1} \alpha^{q^i} = -\mathrm{Tr}(\alpha)$ und $c_n = (-1)^n \prod_{i=0}^{n-1} \alpha^{q^i} = (-1)^n \mathrm{N}(\alpha)$. Die allgemeine Situation beschreibt

1.52. Satz:
Ist $\alpha \in \mathbb{F}_{q^n}$ vom Grad d über $\mathbb{F}_q$, d.h. ist $X^d + \sum_{j=1}^{d} c_j X^{d-j}, c_j \in \mathbb{F}_q$ das Minimalpolynom von α über $\mathbb{F}_q$, so gilt

$$\mathrm{Tr}_{n|1}(\alpha) = -\frac{n}{d} c_1$$

und

$$\mathrm{N}_{n|1}(\alpha) = c_d^{n/d} (-1)^n$$

Beweis. Aus (1.51) folgt $\mathrm{Tr}_{n|1}(\alpha) = \mathrm{Tr}_{d|1}(\mathrm{Tr}_{n|d}(\alpha))$. Da $\alpha \in \mathbb{F}_{q^d}$, d.h. $\alpha^{q^d} = \alpha$, ist $\mathrm{Tr}_{n|d}(\alpha) = \frac{n}{d}\alpha$. Also $\mathrm{Tr}_{n|1}(\alpha) = \mathrm{Tr}_{d|1}(\frac{n}{d}\alpha) = \frac{n}{d}(-c_1)$ (vgl. oben). Die zweite Aussage folgt analog. □

Im Beweis von (1.50)(e) wurde der Kern der Spur betrachtet. Im folgenden sollen die Elemente mit Spur Null und Norm Eins bestimmt werden:

1.53. Satz ("HILBERT 90"):
Im Fall $\mathbb{F}_q \subset \mathbb{F}_{q^n}$ gilt

1. $\mathrm{Tr}(\alpha) = 0$ g.d.w. $\exists \beta \in \mathbb{F}_{q^n} : \alpha = \beta - \beta^q$

2. $\mathrm{N}(\alpha) = 1$ g.d.w. $\exists \beta \in \mathbb{F}_{q^n} : \alpha = \beta/\beta^q$

Beweis. Ist α von der Form $\beta - \beta^q$, so ist $\mathrm{Tr}(\alpha) = \mathrm{Tr}(\beta) - \mathrm{Tr}(\beta^q) = \mathrm{Tr}(\beta) - \mathrm{Tr}(\beta) = 0$ wegen (1.50)(b) und (d). Zur Umkehrung bemerken wir, daß $\wp : \beta \mapsto \beta - \beta^q$ eine lineare Abbildung des $\mathbb{F}_q$-Vektorraumes $\mathbb{F}_{q^n}$ ist. Der Kern von $\wp$ ist gerade $\mathbb{F}_q$, d.h. 1-dimensional. Das Bild von $\wp$ hat Dimension $n-1$: es gibt also q^{n-1} viele Elemente der Form $\beta - \beta^q$. Genauso viele Elemente haben Spur=Null (vgl (1.50)(e)). Mit $\operatorname{im}\wp \subseteq \ker \mathrm{Tr}$ folgt die Behauptung. □

Bemerkung:
Der angegebene Beweis ist nicht konstruktiv: zu gegebenem α ist ein β mit $\beta - \beta^q = \alpha$ nicht erkennbar.

Dem kann abgeholfen werden: HILBERT hat gezeigt, wie man zu β gelangt:

1.54. Lemma:
Sind $\alpha, \theta \in \mathbb{F}_{q^n} \mid \mathbb{F}_q$, so gilt für

$$\beta := \alpha\theta^q + (\alpha + \alpha^q)\theta^{q^2} + \cdots + (\alpha + \alpha^q + \cdots + \alpha^{q^{n-2}})\theta^{q^{n-1}}$$

$$\beta - \beta^q = \alpha(\mathrm{Tr}\,\theta - \theta) - \theta(\mathrm{Tr}\,\alpha - \alpha) \qquad (*)$$

□

Es ist einfach, diese Beziehung nachzurechnen. Hat man nun α mit $\mathrm{Tr}(\alpha) = 0$ gegeben, und kennt man ferner ein Element θ mit $\mathrm{Tr}(\theta) = 1$, so reduziert sich $(*)$ tatsächlich auf $\beta - \beta^q = \alpha$. Die Anwendung, die in der Arithmetik endlicher Körper von Charakteristik 2 wichtig wird, besteht im Lösen *quadratischer* Gleichungen.

1.55. Satz (Quadratische Gleichungen in Charakteristik 2):
Die Gleichung $\alpha X^2 + \beta X + \gamma = 0$ mit $\alpha, \beta, \gamma \in \mathbb{F}_{2^n}$ hat

- genau eine Lösung, falls $\beta = 0$
- keine Lösung, falls $\beta \neq 0$ und $\mathrm{Tr}\left(\frac{\alpha\gamma}{\beta^2}\right) = 1$
- 2 Lösungen, falls $\beta \neq 0$ und $\mathrm{Tr}\left(\frac{\alpha\gamma}{\beta^2}\right) = 0$

Beweis. Ist $\beta = 0$, so ist $X^2 = \gamma/\alpha$ eindeutig lösbar, da σ_2 Automorphismus ist.[‖] Falls $\beta \neq 0$, so wird die Gleichung durch $Y := \frac{\alpha}{\beta}X$ und $\delta := \alpha\gamma/\beta^2$ auf Normalform $Y^2 + Y = \delta$ gebracht. Ist y_0 Lösung dieser Gleichung, dann ist $y_0 + 1$ die zweite Lösung. □

[‖] genauer: $(\gamma/\alpha)^{2^{n-1}}$ ist diese Lösung!

Beim Lösen der Gleichung ist man wegen (1.54) auf die explizite Angabe eines Elements θ mit $\mathrm{Tr}(\theta) = 1$ angewiesen. Ist n *ungerade*, so gilt $\mathrm{Tr}(1) = 1$ und das in (1.54) angegebene Element β ist gleich

$$\tau(\alpha) = \sum_{j=0}^{(n-1)/2} \alpha^{2^{2j}} ,$$

gelegentlich als „Halbspur von α“ bezeichnet. (Tatsächlich gilt: $\tau(\alpha)^2 + \tau(\alpha) = \mathrm{Tr}(\alpha) + \alpha$.) Ist n *gerade*, so ist die Halbspur nutzlos. Als θ wählt man nun in der Liste der Basiselemente der Darstellung $\mathbb{F}_{2^n} \mid \mathbb{F}_2$, etwa $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$, das erste Element mit $\mathrm{Tr}(\alpha_i) = 1$. Wegen (1.50)(e) muß es mindestens ein solches geben.

Beispiel:
Die Gleichung $Y^2 + Y = u$ soll in $\mathbb{F}_{2^n}$ für alle auftretenden $u \in \mathbb{F}_{2^n}$ gelöst werden. Dieses Problem stellt sich z.B. bei der Decodierung binärer zyklischer Codes. Wegen der Linearität von $\wp$ (vgl. (1.53)) reicht es, die Gleichungen für eine Basis $Y^2 + Y = \alpha^i, (0 \le i \le n)$ zu lösen, wobei $\mathbb{F}_{2^n} = \mathbb{F}(\alpha)$. Ist $\theta = \alpha^k$ mit $\mathrm{Tr}(\theta) = 1$ fest gewählt, so löst man die modifizierten Gleichungen durch y_i:

$$y_i^2 + y_i = \begin{cases} \alpha^i & \text{falls } \mathrm{Tr}(\alpha^i) = 0 \\ \alpha^i + \theta & \text{falls } \mathrm{Tr}(\alpha^i) = 1 \end{cases}$$

Ist nun $u = \sum_{i=0}^{n-1} u_i \alpha^i$ vorgelegt, so löst $y = \sum_{i=0}^{n-1} u_i y_i$ die Gleichung $Y^2 + Y = u$ – falls diese lösbar ist. Tatsächlich gilt: $y^2 + y = u + \theta\,\mathrm{Tr}(u)$ (nachrechnen!)

Konkreter Fall:
$n = 4$. α ist Nullstelle von $f = X^4 + X + 1$. $\mathrm{Tr}(1) = 0$, da n gerade ist. $\mathrm{Tr}(\alpha) = 0$, da $c_1 = [X^3]f = 0$ (vgl. (1.52)). Also auch $\mathrm{Tr}(\alpha^2) = 0$ und es bleibt $\mathrm{Tr}(\alpha^3) = 1$. Sei $\theta := \alpha^3$. Die Lösungen

$$y_i^2 + y_i = \begin{cases} \alpha^i & i = 0, 1, 2 \\ 0 & i = 3 \end{cases}$$

sind $y_0 = \alpha^5$, $y_1 = \alpha^7$, $y_2 = \alpha^3$, $y_3 = 0$. Beachte, daß für $u = \sum u_i \alpha^i$ gilt $\mathrm{Tr}(u) = u_3$. Ist A die 4×4-Matrix, deren Zeilen die $y_i, (0 \le i \le 3)$ sind, und $u = [u_0, u_1, u_2, u_3]$, so ist uA eine Lösung der Gleichung $Y^2 + Y = u$, falls $u_3 = 0$. Die zweite Lösung ist $1 + uA$. ◀

Kapitel 2

Grundlegende Algorithmen

2.1 Faktorisierung von Polynomen

In vielen Anwendungen stellte sich das Problem, ein vorgelegtes Polynom $f \in \mathbb{F}_q[X]$ in seine irreduziblen Faktoren zu zerlegen. In der Regel haben die Algorithmen zur Lösung diese Problems als Voraussetzung, daß f in seiner quadratfreien Zerlegung vorliegt. Die Frage, wie diese herzustellen ist, wird im Augenblick zurückgestellt.
Zunächst wird f in Blöcke zerlegt, die jeweils alle Faktoren gleichen Grades beinhalten.
Ist z.B. $f = X^6+2X^5+X^4+X^3+2X \in \mathbb{F}_3[X]$, so stellt $(X^2+X\ ,\ X^4+X^3+X^2)$ die sog. *Distinct-Degree-Zerlegung* von f dar. Die vollständige Zerlegung ist $f = (X)(X+1)(X^2+1)(X^2+X+2)$.
Die verschiedenen "Schichten" erhält man durch ggT-Bildung mit den Polynomen $X^{q^i} - X$, beginnend mit $i = 1$.
Genauer geht man so vor:
Das Polynom $g_1 := \mathrm{ggT}(X^q - X, f)$ besteht aus allen linearen Faktoren in f. Deren Produkt wird abdividiert: f/g_1. Das Polynom $g_2 := \mathrm{ggT}(X^{q^2} - X, f/g_1)$ ist das Produkt aller quadratischen Faktoren in f. Weiter geht es dann mit $f/(g_1 g_2)$ usf.

2.1. Algorithmus:
Distinct-Degree-Faktorisierung
Input: $f \in \mathbb{F}_q[X]\,, \deg(f) = n > 0\,,$ quadratfrei
Output: $(g_1, \ldots, g_s)$ — die DistDeg-Zerlegung von f.
1. $h_0 \leftarrow X$; $f_0 \leftarrow f$; $i \leftarrow 0$
repeat
2. $i \leftarrow i + 1$
$h_i = h_{i-1}^q \operatorname{rem} f$ ** schnelle Exponentiation in $\mathbb{F}_q[X]/(f)$ **

3. $g_i \leftarrow \mathrm{ggT}(h_i - X, f_{i-1})$; $f_i \leftarrow f_{i-1}/g_i$
4. **until** $f_i = 1$
5. $s \leftarrow i$

   return $(g_1, \ldots, g_s)$.

2.2. Satz:
Der Algorithmus (2.1) ist korrekt, d.h. die $i$te Komponente g_i des Ergebnisses ist das Produkt aller irreduziblen Faktoren vom Grad i in f. □

Der nächste Schritt besteht in Zerlegung der g_i, d.h. von Polynomen, deren irreduzible Faktoren alle den gleichen Grad haben. Dieser Schritt wird als *Equal-Degree-Faktorisierung* bezeichnet.

Hierbei behandeln wir zunächst nur den Fall, in dem q *ungerade* ist.
Der vorgestellte Algorithmus von CANTOR und ZASSENHAUS benutzt wesentlich das folgende

2.3. Lemma:
Im Körper $\mathbb{F}_q$, q ungerade, bezeichne $\mathbb{F}_q^{\times\,2}$ die Menge der Quadrate. Dann gilt

(i) $\mathbb{F}_q^{\times\,2}$ ist die Untergruppe in $\mathbb{F}_q^\times$ von Ordnung $(q-1)/2$.

(ii) $\mathbb{F}_q^{\times\,2}$ besteht aus allen Elementen in $\mathbb{F}_q^\times$, die Nullstellen der Gleichung $X^{(q-1)/2} - 1 = 0$ sind.

(iii) für alle $a \in \mathbb{F}_q^\times$ gilt $a^{(q-1)/2} \in \{\pm 1\}$.

Beweis. Der *Quadrierungshomomorphismus*

$$\rho = \begin{cases} \mathbb{F}_q^\times \longrightarrow \mathbb{F}_q^\times \\ a \longmapsto a^2 \end{cases}$$

mit $\ker\rho = \{\pm 1\}$ liefert $F_q^{\times\,2} = \mathrm{im}\,\rho \;\cong\; \mathbb{F}_q^\times / \ker\rho$, d.h. $|\,\mathbb{F}_q^{\times\,2}\,| = \frac{q-1}{2}$.
Andererseits betrachten wir

$$\tau : \begin{cases} \mathbb{F}_q^\times \longrightarrow \mathbb{F}_q^\times \\ a \longmapsto a^{(q-1)/2} \end{cases}$$

Offenbar ist $\mathbb{F}_q^{\times\,2}$ Untergruppe von $\ker\tau$, d.h. $|\ker\tau| \geq \frac{q-1}{2}$. Jeder Erzeuger ζ von $\mathbb{F}_q^\times$ hat aber die Eigenschaft $\zeta^{\frac{q-1}{2}} = -1$. Also ist $\ker\tau \neq \mathbb{F}_q^\times$ und somit $\ker\tau = \mathbb{F}_q^{\times\,2}$. Aus dem Homomorphiesatz für Gruppen folgt schließlich $|\,\mathrm{im}\,\tau| = 2$, d.h. $\mathrm{im}\,\tau = \{\pm 1\}$. □

Wir erklären nun die Idee von ProbSplit, d.h. der Faktorisierung vermittels zufällig gewählter Polynome.

Das Polynom $f \in \mathbb{F}_q[X]$ sei quadratfrei vom Grad n und das Produkt von $2 \leq r = n/d$ vielen irreduziblen Polynomen gleichen Grades d, etwa $f = f_1 \cdots f_r$. Da diese relativ-prim zueinander sind, gilt nach dem Chinesischen Restesatz (CRT)

$$\chi : \; R := \mathbb{F}_q[X]/(f) \quad \longrightarrow \quad \mathbb{F}_q[X]/(f_1) \oplus \cdots \oplus \mathbb{F}_q[X]/(f_r) \quad =: \; R_1 \oplus \cdots \oplus R_r$$

ein Ring-Isomorphismus ist. Die Summanden R_i sind *alle* isomorph zu $\mathbb{F}_{q^d}$.

Zu $a \in R$ bilden wir für $1 \leq i \leq r$ die Projektionen auf die einzelnen Komponenten $\chi_i(a) := a \bmod f_i \in R_i$, sodaß $\chi(a) = (\chi_1(a), \ldots, \chi_r(a))$ gilt.

Offenbar ist $\chi_i(a) = 0$ genau dann, wenn f_i ein Teiler des Polynoms a ist. Ist a derart, daß in dem r-tupel $(\chi_1(a), \ldots, \chi_r(a))$ sowohl Komponenten $= 0$ als auch $\neq 0$ auftreten, so ist $\mathrm{ggT}(a, f)$ ein *nichttrivialer* Teiler von f. Solche günstigen Polynome nennen wir *splittings*.

Man beachte, daß die Komponenten nicht "sichtbar" sind, da die vollständige Faktorisierung von f nicht bekannt ist!

Cantor und Zassenhaus haben 1981 (und unabhängig von ihnen auch Camion 1983) folgende probabilistische Prozedur zum Auffinden solcher *splittings* angegeben:

Zum ungeraden q bilden wir den Exponenten $e := (q^d - 1)/2$. Nach (2.3) ist für $\beta \in R_i^\times (= \mathbb{F}_{q^d}^\times)$ das Ergebnis β^e mit gleicher Wahrscheinlichkeit 1 oder -1. Wählt man $a \in \mathbb{F}_q[X]$ mit $\deg a < n$ und $\mathrm{ggT}(a, f) = 1$ gleichverteilt zufällig, so sind die Komponenten $\chi_1(a), \ldots, \chi_r(a)$ des Vektors $\chi(a)$ unabhängig, gleichverteilte Elemente von $\mathbb{F}_{q^d}^\times$ und $\varepsilon_i := \chi_i(a^e) \in R_i$ ist gleich 1 oder -1 mit Wahrscheinlichkeit 1/2. Das Polynom $a^e - 1$ ist also ein splitting, wenn nicht alle ε_i gleich sind. Oder anders: in dem Vektor

$$\chi(a^e - 1) = (\varepsilon_1 - 1, \ldots, \varepsilon_r - 1).$$

befinden sich Nullen, aber nicht nur Nullen.

Der ungünstige Fall eines konstanten Vektors tritt auf mit Wahrscheinlichkeit $2(\frac{1}{2})^r = 2^{-r+1} \leq \frac{1}{2}$.

2.4. Algorithmus:
Cantor-Zassenhaus (ProbSplit)
Input: $f \in \mathbb{F}_q[X]$ quadratfrei (q ungerade) alle irreduziblen Faktoren von f vom gleichen Grad d. $(d|n, d < n)$
Output: $g \in \mathbb{F}_q[x]$, ein nichttrivialer Teiler von f.
1. Wähle $a \in \mathbb{F}_q[X], \deg(a) < n$ zufällig und nicht konstant.
2. $g_1 \leftarrow \mathrm{ggT}(a, f)$: —falls $g_1 \neq 1$ return g_1
3. Berechne $b := a^{(q^d-1)/2} \operatorname{rem} f \in R$

4. $g_2 \leftarrow \mathrm{ggT}(b-1, f)$
Ist g_2 weder 1 noch f, return g_2 sonst: Fehlversuch.

(*Hinweis:* vgl. Maple: Mathematics ... Algebra ... Polynomials ... Factorization and Root Finding ... ProbSplit)

Beispiel:
Es sei bekannt, daß $f := X^4 + X^3 + X - 1 \in \mathbb{F}_3[X]$ Produkt von 2 irreduciblen Ponynomen vom Grad 2 ist. Man experimentiert in Maple mit verschiedenen a vom Grad ≤ 3:

$$g := \mathsf{Gcd}(f, \mathsf{Powmod}(a, 4, f, X) - 1 \bmod 3) \bmod 3;$$

und findet $f = (X^2 + X - 1)(X^2 + 1)$. Man lese die sehr instruktive Diskussion dieses Beispieles auf den Seiten 362/363 in [3]. ◀

Die folgenden Ausführungen zeigen, wie man die Prämisse "$f \in \mathbb{F}_q[X]$ quadratfrei" erfüllen kann.

2.5. Definition:
Sei R ein kommutativer Ring mit Eins. $D : R[X] \longrightarrow R[X]$ heißt *Ableitung* auf $R[X]$, wenn für $\alpha, \beta \in R$ und $f, g \in R[X]$ gilt: (wir notieren Df als f'):

$$\begin{aligned} (\alpha f + \beta g)' &= \alpha f' + \beta g' \\ (fg)' &= fg' + f'g \\ X' &= 1 \end{aligned}$$

2.6. Lemma:
$f \in \mathbb{F}_q[X]$ habe Grad > 0. Die Ableitung von f ist genau dann Null, wenn $f = g^p$, wobei $p = \mathrm{char}(\mathbb{F}_q)$.

Beweis. $(g^p)' = p \cdot g^{p-1} \cdot g' \equiv 0 \mod p$ besagt, daß die Bedingung hinreichend ist. Ist umgekehrt f mit $f' = 0$ gegeben, etwa

$$f = \sum a_{ip} X^{ip} \quad \text{und} \quad f' = \sum i a_i X^{i-1},$$

so bedeutet dies, daß $p \mid i a_i$, für alle i. Also teilt p alle i mit $a_i \neq 0$, womit f die Gestalt hat :

$$f = \sum_{i=0}^{k} a_{ip} X^{ip}.$$

Der inverse Frobenius-Automorphismus liefert b_i, so daß $b_i^p = a_{ip}$. Also ist f gleich der p-ten Potenz von

$$g = \sum_{i=0}^{k} b_i X^i \ .$$

□

2.7. Satz:
Das Polynom $f \in K[X]$ von positivem Grad ist genau dann quadratfrei, wenn $\mathrm{ggT}(f, f') = 1$ gilt. Das Polynom $g := f/\mathrm{ggT}(f, f')$ ist stets quadratfrei. Die irreduziblen Teiler von g sind die irreduziblen Teiler von f vom Exponenten 1 und diejenigen, deren Exponent *nicht* von der Charakteristik von K geteilt wird.

Beweis. Ist $f = h \cdot j^2$, so folgt aus $f' = j(h'j + 2hj')$, daß $\mathrm{ggT}(f, f') \neq 1$. Ist umgekehrt f quadratfrei und von positivem Grad, so ist nach (2.6) sicher $f' \neq 0$. Sei $d := \mathrm{ggT}(f, f')$ und e so, daß $f = ed$. Da f nicht quadratfrei ist, gilt $\mathrm{ggT}(e, d) = 1$. Aus der Ableitung $f' = ed' + e'd$ folgt $d|d'$, was nur im Fall $d' = 0$ möglich ist. Als Teiler von f ist d jedoch ebenfalls quadratfrei.

Zum Nachweis, daß $f/\mathrm{ggT}(f, f')$ quadratfrei ist, unterscheiden wir in der kanonischen Zerlegung $f = \prod f_i^{e_i}$ nach Exponenten $e > 1$ bzw. $e = 1$, also explizit:

$$f = \prod_{i=1}^{r+s} f_i^{e_i} \text{ mit } e_i > 1 \text{ für } 1 \leq i \leq r, \text{ und } e_{r+1} = \ldots = e_{r+s} = 1$$

Dann erkennt man aus

$$f' = \sum_{i=1}^{r} e_i f_i' \frac{f}{f_i} + \sum_{j=1}^{s} f_{r+j}' \frac{f}{f_{r+j}},$$

daß

$$f_i^{e_i - 1} | \mathrm{ggT}(f, f') \text{ für } 1 \leq i \leq r$$

und

$$f_{r+j} \not| \mathrm{ggT}(f, f') \text{ für } 1 \leq j \leq s.$$

Ferner gilt:

$$f_i^{e_i} | \mathrm{ggT}(f, f') \iff (f_i^{e_i})' = 0$$

Wir sehen daß $f/\mathrm{ggT}(f, f')$ quadratfrei ist; die irreduziblen Teiler dieses Quotienten sind die $f_{r+j} (1 \leq j \leq s)$ und diejenigen $f_j (1 \leq i \leq r)$ deren Exponent e_i *nicht* von der Charakteristik von K geteilt wird. □

2.8. Definition:
Ist $0 \neq f \in K[X]$, so heißt die Zerlegung

$$f = f_1 \cdot f_2^2 \cdot f_3^3 \cdots f_k^k$$

die *quadratfreie Zerlegung* von f, wenn alle f_i quadratfrei und paarweise teilerfremd sind. Ist f normiert, sowie alle f_i normiert, so ist die Zerlegung überdies eindeutig.

In Charakteristik 0 gelten die Regeln

- $\mathrm{ggT}(f, f') = f_2 f_3^2 \dots f_k^{k-1}$
- $f / \mathrm{ggT}(f, f') = f_1 f_2 \dots f_k$.

Die quadratfreie Zerlegung von $f \in K[X]$ wird mit Hilfe des Algorithmus (2.9) hergestellt:

2.9. Algorithmus:
Squarefree-Faktorisierung: SQFF
Input: $0 \neq f(X) \in K[X], p = \mathrm{char}(K)$.
Output: Listen $PL = (f_1 \dots f_k)$.
$EL = (e_1 \dots e_k) = (1, 2, \dots, k)$
1. $PL \leftarrow [\,]$; $EL \leftarrow [\,]$,
2. $g(X) := \mathrm{ggT}(f, f')$, $h(X) := f/g$, $i \leftarrow 1$
3. **while** $h \neq 1$ **do**
   $j(X) = \mathrm{ggT}(g, h)$
   $k(X) = g/j$
   $PL \leftarrow [op(PL), h/j]$
   $EL \leftarrow [op(EL), i]$
   $i \leftarrow k$
   $h \leftarrow j$
   $i \leftarrow i + 1$
4. **if** $\mathrm{char}(K) = 0$ **or** $g' \neq 0$
   then return output $\{PL, EL\}$
5. $g(X) = b(X)^{p^e}$ $\quad **e$ maximal$**$
   $PL \leftarrow [op(SQFF(b)[1], PL]$
   $EL \leftarrow [op(p^e \cdot SQFF(b)[2], EL]$
   return

Von Elwyn R. Berlekamp stammt eine weitere Methode zur Faktorisierung. Die LINEARE ALGEBRA ist dabei die Methode der Wahl!
Man geht wieder von einem quadratfreien normierten Polynom $f \in \mathbb{F}[X]$ vom Grad n aus und untersucht innerhalb von $R = \mathbb{F}[X]/(f)$ eine bestimmte Unteralgebra. Wir betrachten dazu erneut die $\mathbb{F}_q$-lineare Abbildung

$$\wp = \sigma_q - \mathrm{id} : \begin{cases} R \longrightarrow R \\ a \longmapsto a^q - a \end{cases}$$

und untersuchen den Kern von $\wp$. Ist $f = f_1 \cdots f_r$ die Zerlegung von f in irreduzible Faktoren über $\mathbb{F}_q$, so gilt wie oben nach CRT :

$$R \cong \mathbb{F}_q[X]/(f_1) \oplus \dots \oplus \mathbb{F}_q[X]/(f_r) \ .$$

Jede Komponente ist ein Erweiterungskörper von $\mathbb{F}_q$:

$$\mathbb{F}_q[X]/(f_i) \cong \mathbb{F}(q^{d_i}) \ , \quad d_i = \deg(f_i) \ .$$

Der Kern von $\wp$ ist isomorph zu $\underbrace{\mathbb{F}_q \oplus \ldots \oplus \mathbb{F}_q}_{r \text{ mal}}$, d.h. ein r-dimensionaler Vektorraum über $\mathbb{F}_q$; denn

$$\begin{aligned} a \bmod f \in \ker \wp &\iff a^q \equiv a \mod f \\ &\iff a^q \equiv a \mod f_i \qquad \forall_{1\le i\le r} \\ &\iff \quad a \mod f_i \in \mathbb{F}_q \quad \forall_{1\le i\le r} \end{aligned}$$

++++++++++++++++++++B I L D ++++++++++++++++

2.10. Definition:
$\mathcal{B} := \ker \wp$ heißt die BERLEKAMP-Unteralgebra von R.
Wird der FROBENIUS-Automorphismus σ_q bzgl. der Standard-Basis $X^0 \bmod f, X^1 \bmod f, \ldots X^{n-1} \bmod f$ beschrieben, so heißt die darstellende Matrix $Q \in \mathbb{F}_q^{n\times n}$ die PETR-BERLEKAMP-Matrix zu f.

Im BERLEKAMP-Algorithmus wird zunächst eine Basis $b_1 \bmod f, \ldots, b_r \bmod f$ der BERLEKAMP-Algebra $\mathcal{B}$ bestimmt, indem man in $Q - I$ GAUSS-Elimination durchführt. Man beachte daß

$$f \text{ irreduzibel } \iff r = 1 \iff \text{rank } (Q - I) = n - 1.$$

Wieder wird hier zunächst nur der Fall $q \equiv 1 \bmod 2$ behandelt. Im Algorithmus (2.4) wurde der Exponent $\frac{q^d-1}{2}$ zur Erzeugung von $\mathbb{F}_q$-Vektoren bemüht, da R aus lauter gleich großen Komponenten $\mathbb{F}_{q^d}$ bestand. In $\mathcal{B}$ leistet der Exponent $\frac{q-1}{2}$ Entsprechendes. Man wählt ein zufälliges Element $b \in \mathcal{B}$, d.h. Elemente $c_1, \ldots, c_r \ \in \mathbb{F}_q$ zufällig mit $b = c_1 b_1 + \cdots + c_r b_r$, und bildet nach einem Test auf $\text{ggT}(b, f) \stackrel{?}{=} 1$ das Polynom $b^{(q-1)/2} \bmod f$. Falls also $\text{ggT}(b, f) = 1$, so sind die Komponenten $b^{(q-1)/2} \bmod f_i \in \{\pm 1\}$, jeweils mit Wahrscheinlichkeit $\frac{1}{2}$, unabhängig für alle $1 \le i \le r$.

Das ergibt folgenden Algorithmus:

2.11. Algorithmus:
Faktorisierungs Algorithmus (Berlekamp Big Prime)
Input: $f \in \mathbb{F}_q[X], \deg f > 0, f$ quadratfrei, q ungerade.
Output: Entweder ein irreduzibler Faktor von f oder Fehlversuch
1. Berechne $X^q \bmod f$
2. Aufstellen der FROBENIUS-Matrix $Q = (q_{ij}) \in \mathbb{F}_q^{n\times n}$, d.h.
für $0 \le i \le n$ berechne

$$X^{qi} \operatorname{rem} f = \sum_{j=0}^{n-1} q_{ij} X^j$$

3. Via Gauß-Elimination: $r :=$ Rang des Nullraumes der BERLEKAMP-Matrix $B = Q - I \in {\mathbb{F}_q}^{n \times n}$
if $r = 1$ **then return** "*f irreduzibel*"
else $\{b_1 \bmod f, \ldots, b_r \bmod f\}$ Basis des Nullraumes
4. $b := \sum_{i=1}^{r} c_i b_i \quad c_1, \ldots, c_r \in \mathbb{F}_q$ unabhängig, gleichverteilt gewählt.
5. $g_1 \leftarrow \gcd(b, f)$
if $g_1 \neq 1$ **then return** g_1
6. $a \leftarrow b^{\frac{q-1}{2}} \operatorname{rem} f$
7. $g_2 \leftarrow \gcd(a - 1, f)$
if $g_2 \neq 1$ und $g_2 \neq f$ **return** g_2
else *"Fehlversuch"*

N.B. Man beachte, daß (2.11) mit Ergebnis $r = 1$ in 3. einen Irreduzibilitätstest für f darstellt. Weitere Tests vgl. unten.

Beispiel:
Ein Beispiel für (2.11) : $f = X^5 + X^2 + 2X + 1 \in \mathbb{F}_3[X]$.
Frobenius Matrix: $Q = (q_{ij}) \in {\mathbb{F}_3}^{5 \times 5}$; Zeilen bestehen aus $X^{3i} \bmod f, 0 \leq i \leq 4$

$$\begin{array}{lll} X^0 & \bmod f & : \\ X^3 & \bmod f & : \\ X^6 & \bmod f & : \\ X^9 & \bmod f & : \\ X^{12} & \bmod f & : \end{array} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 2 & 1 & 2 & 0 \\ 2 & 2 & 1 & 1 & 2 \\ 2 & 0 & 1 & 0 & 0 \end{pmatrix} = Q$$

Die Berlekamp-Matrix ist $B = Q - I$

$$B = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 & 0 \\ 0 & 2 & 0 & 2 & 0 \\ 2 & 2 & 1 & 0 & 2 \\ 2 & 0 & 1 & 0 & 2 \end{pmatrix}$$

Ein Vektor $(v_0, v_1, v_2, v_3, v_4)$ liegt im Kern von B, wenn gilt : $v_1 = v_2 = v_3$ (2. und 4. Spalte); und $v_3 = -v_4$ (1., 3., 5. Spalte) und ansonsten v_0 beliebig. Also: die normierten Polynome $X^4+2X^3+2X^2+2X$ und $X^4+2X^3+2X^2+2X+1$ bilden eine Basis von $\mathcal{B}$. Der Exponent $\frac{q-1}{2}$ ist hier 1.
Versuche :

$$\begin{aligned} \gcd(a - 1, f) &= X^3 + 2X + 1 \\ \gcd(a + 1, f) &= X^2 + 1 \end{aligned}$$

Ergebnis :

$$f = (X^3 = 2X + 1)(X^2 + 1). \qquad \blacktriangleleft$$

Der dominierende Kostenanteil liegt im Schritt 3 : in der GAUSS-Elimination. Das Verfahren hat eine *deterministische* Variante, deren Rechenaufwand allerdings nicht mehr polynomiell in $\log q$ ist. Andererseits wird der Fall der Charakteristik 2 eingeschlossen. Das entscheidende Hlfsmittel ist

2.12. Lemma:
Ist $b \in \mathbb{F}_q[X]$ so, daß $b \bmod f \in \mathcal{B}$, der BERLEKAMP-Algebra von f, so gilt

$$f = \prod_{\alpha \in \mathbb{F}_p} \mathrm{ggT}(f, b - \alpha)$$

Beweis. Jeder einzelne $\mathrm{ggT}(f, b-\alpha)$ ist Teiler von f. Für $\alpha \neq \beta$ sind diese teilerfremd. Also ist das rechts stehende Produkt Teiler von f.
Ist andererseits $g|f$ ein irreduzibler Faktor, so gilt: $b \equiv \alpha \bmod g,\ \alpha \in \mathbb{F}_q$. Also $g|\,\mathrm{ggT}(f, b-\alpha)$. Da f als quadratfrei vorausgesetzt ist, sind alle irreduziblen Faktoren von f relativ prim zueinander. Somit teilt f das Produkt. Alle betrachteten Polynome sind normiert, so daß die behauptete Gleichheit folgt. □

2.13. Algorithmus:
Berlekamp (Small Prime)
Input: $f \in \mathbb{F}_q[X], \deg f > 0, f$ quadratfrei.
Output: Vollständige Faktorisierung von f.
1. 2. 3. wie in Berlekamp (Big Prime).
4. **für alle** Basisvektoren und **alle** Konstanten in F_q prüfe
$\gcd(f, b - \alpha)$.
5. Liste aller Faktorn von f

Zur Korrektheit dieses Verfahrens wird gezeigt:

2.14. Lemma:
Hat f wenigstens zwei verschiedene normierte irreduzible Faktoren, so liefert der Algorithmus (2.13) einen nichttrivialen Faktor von f.

Beweis. $f_1 \cdots f_r = f$ sei die Zerlegung in irreduzible Faktoren. Der Algorithmus bestimmt Elemente a mit $a^q \equiv a \bmod f$, d.h. $a \in \mathcal{B}$.
Sind in $a = (a^{(1)} \ldots a^{(r)})$ nicht alle $a^{(i)}$ gleich, so etwa $a^{(1)} \neq a^{(2)}$. Verschiebt man a um die Konstante $\alpha = a^{(1)}$, so zeigt

$$\begin{aligned} a - \alpha &= (a^{(1)}, \ldots, a^{(r)}) - (a^{(1)}, \ldots, a^{(1)}) \\ &= (0, a^{(2)} - a^{(1)}, \ldots, a^{(r)} - a^{(1)}) \ , \end{aligned}$$

daß

$$\begin{aligned} a - \alpha &\equiv 0 \bmod f_1 \quad \text{d.h.} \quad f_1 \mid \mathrm{ggT}(a - \alpha) \\ a - \alpha &\not\equiv 0 \bmod f_2 \quad \text{d.h.} \quad f_2 \nmid \mathrm{ggT}(a - \alpha) \ . \end{aligned}$$

Also ist $\mathrm{ggT}(a - \alpha, f)$ ein nichttrivialer Faktor von f. Durchläuft a nun eine Basis $b_1, \ldots, b_r$ von $\mathcal{B}$, so werden alle Faktoren $f_1, \ldots, f_r$ von f getrennt: denn offenbar $\forall\ 1 \leq i, j \leq r \quad i \neq j \quad \exists$ Basis-Element $b \in \{b_1 \ldots b_r\}$ mit $b^{(i)} \neq b^{(j)}$. $\square$

Kapitel 3

Normalbasen

3.1. Definition:
Hat $\alpha \in \mathbb{F}_{q^n}$ die Eigenschaft, daß die Konjugierten $B := \{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}\}$ eine Basis von $\mathbb{F}_{q^n}|\mathbb{F}_q$ bilden, so heißt α ein normales Element. Die Basis B heißt Normalbasis und das Minimalpolynom von α über $\mathbb{F}_q$ ist ein normales (irreduzibles) Polynom $\in \mathbb{F}_q[X]$.

3.2. Beispiel:
Ist $\alpha \in \mathbb{F}_8$ Nullstelle von $X^3 + X^2 + 1$, so ist α normal: $\{\alpha, \alpha^2, \alpha^4\}$ ist eine Basis von $\mathbb{F}_8|\mathbb{F}_2$. Das Polynom $X^3 + X^2 + 1$ ist also ein normales Polynom in $\mathbb{F}_2[X]$. Ist jedoch $\beta \in \mathbb{F}_8$ Nullstelle von $X^3 + X + 1$, so ist β nicht normal, da die Menge der Konjugierten offenbar $\mathbb{F}_2$-abhängig ist : $\beta^4 + \beta^2 + \beta = 0$. ◀

Allgemeiner: Ein Element mit Spur Null ist *nicht* normal.

3.3. Beobachtung:
Der entscheidende Nutzen von Normalbasen besteht darin, daß die Multiplikation gegenüber gewöhnlichen Polynom-Basen vorteilhaft durchführbar ist. Die q-Potenzierung eines Elementes wird durch einen " kostenfreien" Ringshift bewirkt:
Ist $\{\alpha^{q^i}\}_{i=0}^{n-1}$ Normalbasis von $\mathbb{F}_{q^n}|\mathbb{F}_q$ und und hat α die Darstellung

$$\alpha = \sum_{i=0}^{n-1} a_i \alpha^{q^i} \ ,$$

so gilt

$$\alpha^q = \sum_{i=0}^{n-1} a_i^q (\alpha^{q^i})^q = \sum_{i=0}^{n-1} a_i \alpha^{q^{((i+1))}} \ ,$$

wobei $((j))$ bedeutet, daß j mod n zu rechnen ist.

Das erste Ziel wird sein, Existenz und Anzahl von Normalbasen in einer vorgelegten Erweiterung $\mathbb{F}_{q^n}|\mathbb{F}_q$ nachzuweisen. Dazu wird zunächst der Körper $\mathbb{F}_{q^n}$ als *zyklischer* $\mathbb{F}_q[X]$ -*Modul* interpretiert.
Da der Grundkörper $\mathbb{F}_q$ im folgenden fest bleibt, notieren wir den Frobenius Automorphismus $\sigma_q \in \mathrm{Aut}(\mathbb{F}_{q^n}|\mathbb{F}_q)$ kurz mit σ.
Ist $f = \sum_{i=0}^{k} f_i X^i \in \mathbb{F}_q[X]$ und $\alpha \in \mathbb{F}_{q^n}$, so wird durch

$$f(\sigma)(\alpha) = (\sum_{i=0}^{k} f_i \sigma^i)(\alpha) = \sum_{i=0}^{k} f_i \alpha^{q^i}$$

eine Wirkung von $\mathbb{F}_q[X]$ auf $\mathbb{F}_{q^n}$ definiert. Zum Nachweis der Modul-Eigenschaft zeigen wir, daß die Zuordnung

$$\begin{cases} \mathbb{F}_q[X] \to \mathrm{End}(\mathbb{F}_{q^n}) \\ f \quad \longmapsto \quad f(\sigma) \end{cases}$$

ein Ring-Homomorphismus ist.
Die Additivität ist klar:

$$(f+g)(\sigma) = f(\sigma) + g(\sigma)$$

und die Multiplikativität

$$(fg)(\sigma) = f(\sigma) \circ g(\sigma)$$

ergibt sich aus

$$\begin{array}{rcccl} (fg)(\sigma)(\alpha) & = & (\sum_{i,j} f_i g_i \sigma^{i+j})(\alpha) & = & \sum_{i,j} f_i g_j \alpha^{q^{i+j}} \\ & = & \sum_i f_i \sum_j g_j (\alpha^{q^j})^{q^i} & = & \sum_i f_i (\sum_j g_j \alpha^{q^j})^{q^i} \\ & = & f(\sigma)(g(\sigma)(\alpha)) & = & [f(\sigma) \circ g(\sigma)](\alpha) \end{array}$$

3.4. Definition:
Der *Annullator* von α : $\{f \in \mathbb{F}_q[X] : f(\sigma)(\alpha) = 0\} \trianglelefteq \mathbb{F}_q[X]$ ist ein Ideal in dem Hauptidealring $\mathbb{F}_q[X]$. Das normierte Polynom kleinsten Grades im Annullator erzeugt diesen und heißt die *additive Ordnung* von α, i.Z.: $\mathrm{Ord}_q(\alpha)$.

N.B. *Die additive Ordnung ist ein Polynom!*

Der kleine Satz von FERMAT (1.18) hat jetzt die Form:

3.5. Beobachtung:

$$\forall \alpha \in \mathbb{F}_{q^n} : \mathrm{Ord}_q(\alpha) \mid X^n - 1$$

Die normalen Elemente erweisen sich nun als Elemente von größter linearer Ordnung:

3.6. Beobachtung:

$$\alpha \in \mathbb{F}_{q^n} \mid F_q \textbf{ normal} \iff \mathrm{Ord}_q(\alpha) = X^n - 1.$$

Begründung : Die Konjugierten $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ sind genau dann linear abhängig über $\mathbb{F}_q$, wenn ein Polynom $g \in \mathbb{F}_q[X] \setminus \{0\}$ vom Grad $< n$ existiert mit $g(\sigma)(\alpha) = 0$.

Für den folgenden Satz gab HENSEL 1888 erstmals einen kompletten Beweis:

3.7. Satz:
In jeder Körpererweiterung $\mathbb{F}_{q^n} \mid \mathbb{F}_q$ existieren Normalbasen.

Beweis. Sei $X^n - 1 = f_1^{e_1} \cdots f_r^{e_r}$ kanonisch über $\mathbb{F}_q$ zerlegt. Wir geben zu jeder Primärkomponente ein Element entsprechender additiver Ordnung an, d.h.
Behauptung: $\forall_{1 \le i \le r} : \exists \beta_i \in \mathbb{F}_{q^n} : \mathrm{Ord}_q(\beta_i) = f_i^{e_i}$.
Wir definieren $\forall_{1 \le i \le r} \quad h_i := (X^n - 1)/f_i$. Jedes dieser Polynome vom Grad $< n$ hat Elemente in $\mathbb{F}_{q^n} \setminus \{0\}$, die nicht annulliert werden.
Denn angenommen, $\forall \alpha \in \mathbb{F}_{q^n} \quad h_i(\sigma)(\alpha) = 0$, also explizit

$$0 = h_i(\sigma)(\alpha) = \sum_j h_{ij} \alpha^{q^j} \text{ mit } h_i = \sum_j h_{ij} X^j$$

Dann hätte das Polynom $H_i(X) := \sum_j h_{ij} X^{q^j *}$, obwohl vom Grad $\le q^{n-1}$, q^n Nullstellen, was 1.14 widerspräche.
Somit gibt es $\forall_{1 \le i \le r}$ "Nicht-Nullstellen" : $\alpha_i \in \mathbb{F}_{q^n} : h_i(\sigma)(\alpha_i) \neq 0$
Setze nun:

$$\beta_i := \frac{X^n - 1}{f_i^{e_i}}(\sigma)(\alpha_i) \ \in \mathbb{F}_{q^n}.$$

Dieses Element wird von $f_i^{e_i}$ annulliert:

$$f_i^{e_i}(\sigma)(\beta_i) = (X^n - 1)(\sigma)(\alpha_i) = 0.$$

d.h. $\mathrm{Ord}_q(\beta_i) \mid f_i^{e_i}$. Aber kein echter Teiler von $f_i^{e_i}$ annulliert β_i ; denn

$$f_i^{e_i - 1}(\sigma)(\beta_i) = h_i(\sigma)(\alpha_i) \neq 0.$$

nach Wahl von α_i. Die β_i sind also die gesuchten: $\mathrm{Ord}_q(\beta_i) = f_i^{e_i}$. Schließlich setze man $\beta := \beta_1 + \ldots + \beta_r \in \mathbb{F}_{q^n}$ und zeige, daß $\mathrm{Ord}_q(\beta) = X^n - 1$. Nach (3.6) ist β somit normal. □

*man bezeichnet H als das *linear associate* von h

3.8. Beobachtung:
Normalitäts-Kriterium
Ein Element $\beta \in \mathbb{F}_{q^n}$ ist genau dann ein normales Element der Erweiterung $\mathbb{F}_{q^n} \mid \mathbb{F}_q$, wenn für jeden irreduziblen Faktor $f \mid X^n - 1$ gilt : $\left(\frac{X^n-1}{f}\right)(\sigma)(\beta) \neq 0$.

In Analogie zur EULERschen φ-Funktion definieren wir

3.9. Definition:

$$\begin{aligned} \Phi_q(f) &:= |\,\mathbb{F}_q[X]/(f)^\times| \\ &= \#\{g \in \mathbb{F}_q[X];\, \deg g < \deg f \,\&\, \mathrm{ggT}(g,f) = 1\} \end{aligned}$$

3.10. Satz:
Die Anzahl der normalen Elemente in $\mathbb{F}_{q^n} | \mathbb{F}_q$ ist gleich $\Phi_q(X^n - 1)$.

Beweis. Sei $\alpha \in \mathbb{F}_{q^n}$ ein fixiertes normales Element. Wegen der Unabhängigkeit der Konjugierten hat ein beliebiges $\beta \in \mathbb{F}_{q^n}$ die eindeutige Darstellung

$$\beta = g_0\alpha + g_1\alpha^q + \ldots + g_{n-1}\alpha^{q^{n-1}} = g(\sigma)(\alpha)$$

mit $g := \sum g_i X^i$ und $\deg(g) \leq n-1$.
Die Zuordnung $g \leftrightarrow g(\sigma)(\alpha)$

$$\mathbb{F}_q[X]^{<n} \longleftrightarrow \mathbb{F}_{q^n}$$

ist bijektiv. Tatsächlich zeigen wir die interessantere, eingeschränkte Bijektion:

$$\mathbb{F}_q[X]/(X^n-1)^\times \longleftrightarrow \{\text{normale Elemente}\}$$

"$\Longleftarrow$" Sei β normal, d.h. $\mathrm{Ord}_q(\beta) = X^n - 1$, mit der Darstellung $\beta = g(\sigma)(\alpha)$. Sei $t := (X^n-1)/\,\mathrm{ggT}(g, X^n-1)$. Damit folgt $X^n - 1 \mid t \cdot g$ und wegen (3.5) $0 = t(\sigma)g(\sigma)(\alpha) = t(\sigma)(\beta)$. Da β normal ist, folgt $X^n - 1 \mid t$, was nach Definition von t notwendig $\mathrm{ggT}(g, X^n-1) = 1$ impliziert.
"$\Longrightarrow$" Es sei ein g mit $\mathrm{ggT}(g, X^n-1) = 1$ gegeben, und β sei das zugehörige Element : $\beta = g(\sigma)(\alpha)$. Daß β von seiner additiven Ordnung annulliert wird heißt : $0 = \mathrm{Ord}_q(\beta)(\sigma)(\beta) = (\mathrm{Ord}_q(\beta) \cdot g)(\sigma)(\alpha)$. Da α als normal vorausgesetzt war, folgt $X^n - 1 \mid \mathrm{Ord}_q(\beta) \cdot g$, was wegen $\mathrm{ggT}(g, X^n-1) = 1$ zur Folge hat : $X^n - 1 \mid \mathrm{Ord}_q(\beta)$. Somit ist β normal. □

Zur Berechnung von $\Phi_q(f)$:

Hat f die kanonische Faktorisierung $f = \prod_{i=1}^r f_i^{e_i}$, so liefert der Chinesische Restesatz die Ringisomorphie

$$\mathbb{F}_q[X]/(f) \cong \bigoplus_{i=1}^{r} (\mathbb{F}_q[X]/(f_i^{e_i}))$$

Diese Ringisomorphie induziert eine Gruppenisomorphie der entsprechenden Einheitengruppen:

$$\mathbb{F}_q[X]/(f)^\times \cong \bigotimes_{i=1}^{r} \mathbb{F}_q[X]/(f_i^{e_i})^\times$$

woraus die Multiplikativität von Φ_q folgt:

$$\Phi_q(f) = \prod_{i=1}^{r} \Phi_q(f_i^{e_i})$$

In jeder Komponente gilt: $\mathrm{ggT}(g, f_i^{e_i}) = 1 \iff f_i \nmid g$. Mit einer Notation für die "Größe" von f, nämlich $|f| = q^{\deg(f)} =\mid \mathbb{F}_q[X]/(f) \mid$ erhält man für die Einheitengruppe einer einzelnen Primärkomponente:

$$\mid \mathbb{F}_q[X]/((f_i^{e_i})^\times \mid = \; |f_i^{e_i}| - |f_i^{e_i-1}| \; = \; |f_i^{e_i}| \cdot (1 - \frac{1}{|f_i|})$$

Mit der Bezeichnung

$$\mathcal{I}_q := \{g \in \mathbb{F}_q[X]; g \text{ irred \& normiert}\}$$

erhalten wir nun:

$$\begin{aligned} \Phi_q(f) &= \prod_{i=1}^{r} \Phi_q(f_i^{e_i}) \\ &= \prod_{i=1}^{r} |f_i^{e_i}|(1 - \frac{1}{|f_i|}) \\ &= \prod_{i=1}^{r} |f_i^{e_i}| \prod_{i=1}^{r} (1 - \frac{1}{|f_i|}) \end{aligned}$$

$$\Phi_q(f) = |f| \prod_{\substack{g \in \mathcal{I}_q \\ g|f}} (1 - \frac{1}{|g|}) \tag{3.1}$$

in völliger Analogie zur bekannten Formel für die EULERsche φ-Funktion:

$$\varphi(n) = n \cdot \prod_{\substack{p \text{ prim} \\ p|n}} (1 - \frac{1}{p})$$

Beispiel:
$q = 2$; $f = X^6 - 1$. $\Phi_2(X^6 - 1) = \#\{$ normale Elemente in $\mathbb{F}_{64} \mid \mathbb{F}_2\}$. Die Zerlegung von $X^6 - 1$ in $\mathbb{F}_2[X]$ ist leicht zu sehen:

$$X^6 + 1 = (X^3 + 1)^2 = (X + 1)^2(X^2 + X + 1)^2$$

$$\Phi_2(X^6-1) = 2^6(1-\frac{1}{2})(1-\frac{1}{4}) = 24$$

Die 24 normalen Elemente bilden 4 Klassen zu je 6 Konjugierten, d.h. es gibt $\frac{1}{6}\Phi_2(X^6-1) = 4$ *normale* Polynome von Grad 6 über $\mathbb{F}_2$:

$$X^6+X^5+1, \quad X^6+X^5+X^4+X+1, \quad X^6+X^5+X^2+X+1,$$

$$X^6+X^5+X^4+X^2+1.$$

Die ersten 3 sind außerdem primitiv. (Hinweis: detaillierte Informationen über den Körper $\mathbb{F}_{64}$ findet man in [6], **Table B**. Zur Übung möge man die normalen Polynome dort identifizieren!) ◀

Die Formel (3) zeigt, daß in die Berechnung von $\Phi_q(f)$ lediglich die Grade der irreduziblen Teiler von f eingehen. Tatsächlich können wir für die Anzahl der normalen Elemente eine Formel beweisen, in der nur Funktionen aus der elementaren Zahlentheorie angesprochen werden:

3.11. Satz:
Es sei $\mathbb{F}_{q^n} \mid \mathbb{F}_q$ eine Körpererweiterung von Grad n und Charakteristik p. Ist $n = p^e \cdot n'$ mit $\mathrm{ggT}(n',p) = 1$ und bezeichnet $\nu(n,q)$ die Anzahl der normalen Elemente dieser Erweiterung, so gilt

$$\nu(n,q) = q^{n-n'} \prod_{d|n'} (q^{\mathrm{ord}_d(q)} - 1)^{\varphi(d)/\,\mathrm{ord}_d(q)} \quad .$$

Beweis. Wegen Charakteristik p gilt in $\mathbb{F}_q[X]$:

$$X^n - 1 = (X^{n'} - 1)^{p^e}$$

Wir wissen nach (1.41)

$$X^{n'} - 1 = \prod_{d|n'} Q_d(X)$$

wobei $Q_d(X)$ quadratfrei über $\mathbb{F}_q$ und vom Grad $\varphi(d)$. Ferner haben wir die wichtige Information (1.42): $Q_d(X)$ zerfällt in $\varphi(d)/\,\mathrm{ord}_d(q)$ viele irreduzible Faktoren vom Grad $\mathrm{ord}_d(q)$. Demnach gilt (beachte, daß $\sum_{d|n'} \varphi(d) = n'$)

$$\begin{aligned} \nu(n,q) &= q^n \prod_{d|n'} (1 - \frac{1}{q^{\mathrm{ord}_d(q)}})^{\varphi(d)/\,\mathrm{ord}_d(q)} \\ &= q^{n-n'} \prod_{d|n'} (q^{\mathrm{ord}_d(q)} - 1)^{\varphi(d)/\,\mathrm{ord}_d(q)} \end{aligned}$$

□

Beispiel:
Im obigen Beispiel führt das zu der vereinfachten Rechnung:
$n = 6; n' = 3$ und $q = 2$. $\mathrm{ord}_1(2) = 1; \mathrm{ord}_3(2) = 2$
Also: $\nu(6,2) = 2^{6-3}(2^1-1)^1(2^2-1)^1 = 8 \cdot 1 \cdot 3 = 24$ ◀

Die Formel in (3.11) gibt keinen Aufschluss über die Dichte von normalen Elementen. Eine (universelle) untere Schranke für diese hat GUDMUND S. FRANDSEN in [2] gezeigt:

3.12. Satz:
Für jeden Körper $\mathbb{F}_{q^n}$ gilt für die Anzahl $\nu(q,n)$ der über $\mathbb{F}_q$ normalen Elemente

$$\frac{\nu(q,n)}{q^n} \geq \frac{1}{e \cdot \lceil \log_q n \rceil}$$

Nachdem nun Existenz, Anzahl und Dichte von normalen Elementen behandelt sind, wollen wir die eingangs gemachten Bemerkung (3.3) vertiefen.
Ist $\alpha = \alpha_0, \alpha^q = \alpha_1, \ldots, \alpha^{q^{n-1}} = \alpha_{n-1}$ eine Normalbasis von $\mathbb{F}_{q^n}|\mathbb{F}_q$, so beschreibt die Entwicklung

$$\alpha\alpha_i = \sum_{j=0}^{n-1} t_{ij}\alpha_j, \ 0 \leq i \leq n-1, \ t_{ij} \in F_q. \quad (*)$$

die Multiplikation von *je zwei* Basiselementen vollständig (Beweis ?). Die Matrix $(t_{ij}) \in \mathbb{F}_q^{n \times n}$ werde mit T bezeichnet.

3.13. Definition:
Nach Mullin, Onyszchuk, Vanstone und Wilson nennen wir die Anzahl der Einträge $\neq 0$ in T die *Komplexität* der Normalbasis N, i.Z. c_N. Die Matrix T heißt die *Multiplikations-Tafel* der Normalbasis.

Der folgende Satz liefert eine untere Schranke für c_N, die sich als scharf herausstellen wird.

3.14. Satz:
Für jede Normalbasis N von F_{q^n} über F_q gilt $c_N \geq 2n-1$.

Beweis. Sei $N = \{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ eine Normalbasis von $\mathbb{F}_{q^n}$ über $\mathbb{F}_q$. Dann ist $\sum_{i=0}^{n-1} \alpha_i = \mathrm{Tr}(\alpha) \in \mathbb{F}_q$. Summiert man die Gleichungen $(*)$ über i so liefert der Koeffizientenvergleich

$$\sum_{i=0}^{n-1} t_{ij} = \begin{cases} \mathrm{Tr}(\alpha) & j = 0, \\ 0 & 1 \leq j \leq n-1. \end{cases}$$

Da $\alpha \neq 0$, ist $\{\alpha \cdot \alpha_i : 0 \leq i \leq n-1\}$ ebenfalls eine Basis F_{q^n} von F_n. Daher ist die Matrix $T = (t_{ij})$ invertierbar. Für jedes j ist also mindestens ein $t_{ij} \neq 0$. Überdies müssen für jedes $j \neq 0$ mindestens zwei Elemente $t_{ij} \neq 0$ sein, damit sich die Spalte zu Null summiert. Es gibt also mindestens $2(n-1)+1 = 2n-1$ von Null verschiedene Elemente in T. □

3.15. Definition:
Eine Normalbasis N heißt *optimal*, wenn $c_N = 2n-1$ gilt.

Dem Buch [8] folgend werden wir nun ein Theorem (3.17) beweisen, das die Existenz optimaler Normalbasen sicherstellt.
Das folgende technische Lemma wird den Beweis dieses Theorems übersichtlicher gestalten:

3.16. Lemma:
Seien k, n ganze Zahlen, so daß $nk+1$ prim ist, und sei die Ordnung von q modulo $(nk+1)$ gleich e. Angenommen, $\mathrm{ggT}(nk/e, n) = 1$. Sei ferner τ eine primitive k-te Einheitswurzel in $\mathbb{Z}_{nk+1}$. Dann hat jedes Element $\rho \neq 0$ in $\mathbb{Z}_{nk+1}$ die eindeutige Darstellung

$$\rho = \tau^i q^j, \quad 0 \leq i \leq k-1, \quad 0 \leq j \leq n-1.$$

Beweis. Sei $e_1 = nk/e$. Dann gibt es ein primitives Element g in $\mathbb{Z}_{nk+1}^{\times}$ so, daß $q = g^{e_1}$. Da g die Ordnung nk hat und τ die Ordnung k, gibt es eine ganze Zahl a mit $\mathrm{ggT}(a,k) = 1$ so daß $\tau = g^{na}$. Damit sind q und τ bzgl. einer geeigneten Primitivwurzel dargestellt. Nun, angenommen es gibt $0 \leq i, s \leq k-1$ und $0 \leq j, t \leq n-1$, so daß

$$\tau^i q^j \equiv \tau^s q^t \pmod{nk+1},$$

i.e.

$$\begin{aligned} \tau^{i-s} &\equiv q^{t-j} \pmod{nk+1}, \\ g^{na(i-s)} &\equiv g^{e_1(t-j)} \pmod{nk+1}. \end{aligned}$$

Dann

$$na(i-s) \equiv e_1(t-j) \mod nk \qquad (\dagger)$$

Da $\gcd(n, e_1) = 1$ ist, muß $n \mid (t-j)$ gelten, also $t = j$. Aus $(\dagger)$ folgt nun

$$a(i-s) \equiv 0 \pmod{k}.$$

Aber $\gcd(a,k) = 1$, so daß $k \mid (i-s)$. Daher $i = s$. Dies beweist, daß die kn Elemente

$$r^i q^j \bmod (nk+1), \ i = 0, 1, \ldots, k-1, \ j = 0, 1, \ldots, n-1$$

ganz $\mathbb{Z}_{nk+1}^{\times}$ erschöpfen. □

3.17. Theorem:
Seien q eine Primzahl oder eine Primpotenz und $nk+1$ eine Primzahl, die q nicht teilt $(n, k \in \mathbb{N})$. Sei β eine primitive $(nk+1)$te Einheitswurzel in $\mathbb{F}_{q^{nk}}$. Für die Ordnung e von q mod $(nk+1)$ sei ggT$(nk/e, n) = 1$ vorausgesetzt. Für jede primitive k-te Einheitswurzel $\tau \in \mathbb{Z}_{nk+1}$ erzeugt dann die GAUSS-*Periode*

$$\alpha = \sum_{i=0}^{k-1} \beta^{\tau^i}$$

eine Normalbasis von $\mathbb{F}_{q^n}|\mathbb{F}_q$ mit einer Komplexität von höchstens $(k+1)n - k$. Im Falle $k \equiv 0 \bmod p$ ist diese höchstens $kn - 1$, wobei p die Charakteristik des Körpers ist.

Beweis. Zuerst beweisen wir, daß $\alpha \in F_{q^n}$. Da $q^{nk} \equiv 1 \bmod (nk+1)$, ist q^n eine k-te Einheitswurzel in $\mathbb{Z}_{nk+1}$. Es gibt demnach eine ganze Zahl l, so daß $q^n = \tau^l$.

$$\alpha^{q^n} = \sum_{i=0}^{k-1} \beta^{\tau^i q^n} = \sum_{i=0}^{k-1} \beta^{\tau^{i+l}} = \sum_{i=0}^{k-1} \beta^{\tau^i} = \alpha.$$

Als nächstes wird bewiesen, daß $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ $\mathbb{F}_q$-linear unabhängig sind. Dazu nehmen wir an, daß eine $\mathbb{F}_q$-Abhängigkeit existiert von der Gestalt

$$\sum_{i=0}^{n-1} \lambda_i \alpha^{q^i} = \sum_{i=0}^{n-1} \lambda_i \sum_{j=0}^{k-1} \beta^{\tau^j q^i} = 0$$

Beachte, daß für jede $(nk+1)$te Einheitswurzel γ eindeutig bestimmte $u_i \in \mathbb{F}_q$, $(i = 1, 2, \ldots, kn)$ existieren mit

$$\sum_{i=0}^{n-1} \sum_{j=0}^{k-1} \lambda_i \gamma^{\tau^j q^i} = \sum_{j=1}^{nk} u_j \gamma^j = \gamma \sum_{j=0}^{nk-1} u_{j+1} \gamma^j,$$

weil nach (3.16) $\tau^j q^i \bmod (nk+1)$ für $j = 0, 1, \ldots, k-1$ und $i = 0, 1, \ldots, n-1$ ganz $\mathbb{Z}^*_{nk+1}$durchläuft.
Sei $f(X) = \sum_{j=0}^{nk-1} u_{j+1} X^j$ das "generische" Polynom. Für jedes $1 \le \rho \le nk$ existieren ganze Zahlen u und v, derart, daß $\rho = \tau^u q^v$. Da β^ρ ebenfalls eine $(nk+1)$te primitve Einheitswurzel ist, ergibt sich

$$\begin{aligned} \beta^\rho f(\beta^\rho) &= \sum_{i=0}^{n-1} \lambda_i \sum_{j=0}^{k-1} (\beta^\rho)^{\tau^j q^i} = \sum_{i=0}^{n-1} \lambda_i \left(\sum_{j=0}^{k-1} \beta^{\tau^{u+j} q^i} \right)^{q^v} \\ &= \left(\sum_{i=0}^{n-1} \lambda_i \sum_{j=0}^{k-1} \beta^{\tau^j q^i} \right)^{q^v} = 0, \end{aligned}$$

daß alle β^ρ $(\rho = 1, 2, \ldots, nk)$ Wurzeln von $f(x)$ sind.
Der Grad von f ist aber höchstens $nk-1$!
Als nächstes berechnen wir die Multiplikationstabelle dieser Basis. Beachte, daß für $0 \le i \le n-1$ gilt

$$\begin{aligned}\alpha \cdot \alpha^{q^i} &= \sum_{u=0}^{k-1}\sum_{v=0}^{k-1} \beta^{\tau^u+\tau^v q^i} = \sum_{u=0}^{k-1}\sum_{v=0}^{k-1} \beta^{\tau^u(1+\tau^{v-u}q^i)} \\ &= \sum_{v=0}^{k-1}\left(\sum_{u=0}^{k-1} \beta^{\tau^u(1+\tau^v q^i)}\right) \qquad (\ddagger)\end{aligned}$$

Es gibt ein eindeutig bestimmtes Paar $(v_0, i_0), 0 \le v_0 \le k-1,\ 0 \le i_0 \le n-1$ derart, daß $1+\tau^{v_0}q^{i_0} \equiv 0 \bmod (nk+1)$. Wenn $(v,i) \ne (v_0,i_0)$, dann ist $1+\tau^v q^i \equiv \tau^w q^j \bmod (nk+1)$, für $0 \le w \le k-1,\ 0 \le j \le n-1$, und

$$\sum_{u=0}^{k-1} \beta^{\tau^u(1+\tau^v q^i)} = \sum_{u=0}^{k-1} \beta^{\tau^{u+w}q^j} = \left(\sum_{u=0}^{k-1} \beta^{\tau^u}\right)^{q^j} = \alpha^{q^j}.$$

Wenn jedoch $(v,i) = (v_0,i_0)$, dann ist

$$\sum_{u=0}^{k-1} \beta^{\tau^u(1+\tau^v q^i)} = k,$$

was gleich 0 ist, falls $k \equiv 0 \bmod p$. Also: für alle $i \ne i_0$ ist die Summe $(\ddagger)$ eine Summe von höchstens k Basiselementen. Daher ist die Komplexität der Basis höchstens $(n-1)k + n = (k+1)n - k$.
Ist $k \equiv 0 \bmod p$ und $i = i_0$, dann ist $(\ddagger)$ eine Summe von höchstens $k-1$ Basiselementen. Im Fall $k \equiv 0 \bmod p$ ist demnach die Komplexität der Basis höchstens $(n-1)k + k - 1 = kn - 1$. Damit ist der Beweis abgeschlossen. □

Als einen Spezialfall $(k=1)$ erhält man die sog. *Normalbasen vom Typ I :*

3.18. Satz:
Optimale Normalbasen vom Typ I
Es seien $n+1$ eine Primzahl und q ein primitives Element in $\mathbb{F}_{n+1}$, wobei q selbst eine Primzahl oder eine Primpotenz ist. Dann sind die n von 1 verschiedenen $(n+1)$ten Einheitswurzeln in $\mathbb{F}_{q^n}$ linear unabhängig und bilden eine optimale Normalbasis von $\mathbb{F}_{q^n}$ über $\mathbb{F}_q$.

Beweis. Sei β eine primitive $(n+1)$te Einheitswurzel, d.h. Nullstelle des Kreisteilungspolynoms $Q_{n+1}(X) = X^n + \cdots + X + 1$. Dieses ist nach (1.42) irreduzibel über $\mathbb{F}_q$, weil $\varphi(n+1)/\operatorname{ord}_{n+1}(q) = n/n = 1$. Demnach sind alle $(n+1)$ten Einheitswurzeln in $\mathbb{F}_{q^n}$. Die Menge der Potenzen von $\{\beta, \beta^2, \ldots, \beta^n\}$ stimmt somit

überein mit der Menge der Konjugierten $N = \{\beta, \beta^q, \ldots, \beta^{q^{n-1}}\}$. In Übereinstimmung mit dem Theorem (3.17) ist β ein normales Element (die GAUSS-Periode ist für $k = \tau = 1$ besonders einfach!). Das Theorem (3.17) liefert die obere Schranke $c_N \leq 2n-1$, so daß mit (3.14) die Gleichheit folgt: N ist optimal. Daß tatsächlich $c_N = 2n-1$ gilt , ersieht man auch sofort aus

$$\alpha\alpha^i = \alpha^{i+1} \in N, \qquad 1 \leq i < n,$$

und

$$\alpha\alpha^n = 1 = -\operatorname{Tr}(\alpha) = -\sum_{i=1}^{n} \alpha^i.$$

□

N.B. Die optimalen Normalbasen vom *Typ II* entsprechen dem Fall $k = q = 2$ im Theorem (3.17). Es wurde von XUHONG GAO und HENDRIK W. LENSTRA überdies gezeigt, daß damit alle Möglichkeiten des Vorkommens optimaler Normalbasen erschöpft sind. Die genauen Resultate sind authentisch in [8] dargestellt.

3.19. Beispiel:
Es sei in (3.18) $n = 2$ und $p \equiv 2 \bmod 3$ eine Primzahl. Dann ist offenbar p mod 3 primitiv in $\mathbb{F}_3$. Also ist das 3te Kreisteilungspolynom $Q_3(X) = (X^3-1)/(X-1) = X^2 + X + 1$ irreduzibel über $\mathbb{F}_p$ und die beiden Nullstellen α und $\alpha^2 = \alpha^p$ in $\mathbb{F}_{p^2}$ bilden eine optimale Normalbasis vom Typ I in $\mathbb{F}_{p^2}|\mathbb{F}_p$. Die Elemente in $\mathbb{F}_{p^2}$ haben die Darstellung $x_1\alpha + x_2\alpha^2$, wo $x_i \in \mathbb{F}_p$. Beachte, daß die Konstanten $t \in \mathbb{F}_p$ die Darstellung $-t\alpha - t\alpha^2$ haben. Wie allgemein bei Normalbasen ist die p-Potenzierung ein ring-shift, d.h. hier die Vertauschung der zwei Koordinaten:

$$(x_1\alpha + x_2\alpha^2)^p = x_2\alpha + x_1\alpha^2$$

Bemerkenswert ist auch, daß man mit zwei Multiplikationen quadrieren kann:

$$(x_1\alpha + x_2\alpha^2)^2 = x_2(x_2 - 2x_1)\alpha + x_1(x_1 - 2x_2)\alpha^2$$

Weitere Bemerkungen zur Arithmetik in dieser Darstellung siehe [5]. ◄

Literaturverzeichnis

[1] Johann Cigler: *Körper, Ringe, Gleichungen*, Spektrum, 1995

[2] Gudmund S. Frandsen : *On the density of normal bases in finite fields*, erscheint in *Finite Fields and Their Applications* **6** (2000) 23-38 (ps-file: http://www.brics.dk/ gudmund/)

[3] Joachim von zur Gathen, Jürgen Gerhard: *Modern Computer Algebra*, Cambridge University Press, 1999

[4] Serge Lang: *Algebra*, Addison-Wesley, 1993[3]

[5] Arjen K. Lenstra, Eric R. Verheul :(preprint) *The XTR public key system*, http://www.ecstr.com/ (to appear at Crypto 2000)

[6] Rudolf Lidl, Harald Niederreiter: *Finite Fields*, Cambridge University Press, 1997[2]

[7] Heinz Lüneburg: *Galoisfelder, Kreisteilungskörper und Schieberegisterfolgen*, BI, 1979

[8] Alfred J. Menezes (Ed.), Ian F. Blake ... [et al.]: *Applications of Finite Fields*, Kluwer Acad., 1993