Ruprecht-Karls-Universität Heidelberg
Mathematisches Institut

Endliche Körper

Proseminar Endliche Körper, Dr. Denis Vogel

von

Martin Lüdtke
Mathematik (BSc)
Luedtke@stud.uni-heidelberg.de
Matr.-Nr. 2833023

Philipp Siehr
Mathematik (BSc)
P.Siehr@stud.uni-heidelberg.de
Matr.-Nr. 2772186

20. Mai 2010

Wie der Titel des Proseminars sowie der unseres Vortrages vermuten lässt, wollen wir uns mit der Theorie der endlichen Körper befassen. Wir werden zeigen, dass ein endlicher Körper stets p^n Elemente besitzt, wobei p eine Primzahl und $n \in \mathbb{N}$ ist, und dass für jede Wahl von p und n ein (bis auf Isomorphie) eindeutig bestimmter Körper der Ordnung p^n existiert. Wir werden mit Hilfe der Vorbetrachtungen ein allgemeines Verfahren zur Konstruktion endlicher Körper angeben können und exemplarisch den $\mathbb{F}_4$ konstruieren. Ferner werden wir sehen, wie endliche Körper ineinander eingebettet werden können. Abschließend soll unsere Aufmerksamkeit der Betrachtung von n-ten Einheitswurzeln gewidmet sein.

Satz 1. *Sei K ein endlicher Körper der Charakteristik p, so besitzt K genau p^n Elemente, wobei $n = [K : \mathbb{F}_p]$.*

Beweis. Den Körper K kann man als Vektorraum über seinem Primkörper $\mathbb{F}_p$ betrachten, der nach Satz 1.4 Vortrag „Körpererweiterungen II“ bzw. „Satz 1.19 c)“ im Skript, eine endliche Basis von n Elementen besitzt. Jedes Element unseres Körpers K lässt sich bekanntlich als eindeutig bestimmte Linearkombination der n Basisvektoren mit Koeffizienten aus $\mathbb{F}_p$ darstellen. Daher gibt es exakt p^n Elemente in K. □

Definition 2. $(G, \cdot)$ Gruppe. Wenn es für $a \in G$ eine natürliche Zahl n mit $a^n = 1$ gibt, sagen wir, a sei von endlicher Ordnung und nennen das kleinste solche n die *Ordnung* von a ($\mathrm{ord}(a)$). Anderenfalls habe a unendliche Ordnung.
Ist G endlich und existiert ein $a \in G$, so dass G gerade aus den Elementen $1, a, a^2, \ldots, a^{m-1}$ mit $m = \mathrm{ord}(a)$ besteht, so heißt G *zyklisch* und a heißt ein *erzeugendes Element* von G.

Lemma 3. *$(G, \cdot)$ abelsche Gruppe, $a \in G$ mit endlicher Ordnung m, $n \in \mathbb{Z}$. Dann gilt: $a^n = 1 \Leftrightarrow m \mid n$.*

Beweis.

($\Leftarrow$) Gelte $m \mid n$, d. h. $n = km$ für ein $k \in \mathbb{Z}$. Dann folgt $a^n = a^{km} = (a^m)^k = 1^k = 1$.

($\Rightarrow$) Wir können n schreiben als $n = km + r$, wobei $k, r \in \mathbb{Z}$ und $0 \leq r < m$. Gelte nun $a^n = 1$. Dann folgt $1 = a^{km+r} = a^{km}a^r = a^r$ und somit $r = 0$ wegen $0 \leq r < m$ und der Minimalität von $m = \mathrm{ord}(a)$. □

Lemma 4. *$(G, \cdot)$ abelsche Gruppe, $a, b \in G$ Elemente endlicher Ordnung,* $\mathrm{ord}(a)$ *und* $\mathrm{ord}(b)$ *teilerfremd. Dann gilt* $\mathrm{ord}(ab) = \mathrm{ord}(a)\,\mathrm{ord}(b)$.

Beweis. Sei $m := \mathrm{ord}(a)$, $n := \mathrm{ord}(b)$, $\mathrm{ggT}(m, n) = 1$. Ist $\mathrm{ord}(ab) = t$, dann gilt $a^{nt} = a^{nt}b^{nt} = (ab)^{nt} = 1$ und somit $m \mid nt$ nach Lemma 3. Wegen n, m teilerfremd folgt $m \mid t$. Analog erhält man $n \mid t$, es gilt daher $mn \mid t$. Andererseits gilt $(ab)^{mn} = (a^m)^n(b^n)^m = 1$ und somit $t \mid mn$. Daraus folgt die Behauptung. □

Lemma 5. *$(G, \cdot)$ abelsche Gruppe, $a, b \in G$ endlicher Ordnung,* $\mathrm{ord}(a) = m, \mathrm{ord}(b) = n$. *Dann existiert ein Element aus G der Ordnung* $\mathrm{kgV}(m, n)$.

Beweis. Sei $p_1^{\nu_1} \cdots p_r^{\nu_r}$ eine Primfaktorzerlegung von $\mathrm{kgV}(m,n)$. Definiere nun

$$m_0 := \prod_{\substack{i=1 \\ p_i^{\nu_i} \mid m}}^{r} p_i^{\nu_i} \quad \text{und} \quad n_0 := \prod_{\substack{i=1 \\ p_i^{\nu_i} \nmid m}}^{r} p_i^{\nu_i}.$$

Offensichtlich sind m_0 und n_0 teilerfremd und es gilt $m_0 n_0 = \mathrm{kgV}(m,n)$. Ferner gilt $m_0 \mid m$ und $n_0 \mid n$, d. h. es existieren $m', n' \in \mathbb{N}$ mit $m = m_0 m'$, $n = n_0 n'$. Es gilt nun $\mathrm{ord}(a^{m'}) = m_0$ und $\mathrm{ord}(b^{n'}) = n_0$. Wegen der Teilerfremdheit von m_0 und n_0 folgt mit Lemma 4 $\mathrm{ord}(a^{m'} b^{n'}) = m_0 n_0 = \mathrm{kgV}(m,n)$. □

Satz 6. *K Körper, H endliche Untergruppe der multiplikativen Gruppe $(K^\times, \cdot)$. Dann ist H zyklisch.*

Beweis. Da H endlich ist, existiert ein $a \in H$ mit maximaler Ordnung m. Sei H_m die Menge aller Elemente aus H, deren Ordnung m teilt. Dann sind alle Elemente von H_m Nullstellen des Polynoms $X^m - 1$, so dass H_m höchstens m Elemente enthalten kann. Andererseits sind die m Elemente $1, a, \ldots, a^{m-1}$ alle in H_m enthalten, wie man mit Hilfe von Lemma 3 leicht sieht, somit ist $H_m = \{1, a, \ldots, a^{m-1}\}$ die von a erzeugte Untergruppe von H. Wir zeigen, dass nun $H_m = H$ gilt. Gibt es nämlich ein Element $b \in H$, dessen Ordnung m nicht teilt, dann enthält H nach Lemma 5 ein Element der Ordnung $\mathrm{kgV}(m,n) > m$, im Widerspruch zur Maximalität von $\mathrm{ord}(a) = m$. □

Folgerung 7. *Ist K ein endlicher Körper mit q Elementen, dann ist die multiplikative Gruppe $(K^\times, \cdot)$ zyklisch. Alle Elemente k von K genügen der Gleichung $k^q - k = 0$.*

Beweis. Die erste Behauptung folgt direkt aus Satz 6. Ist $a \in K^\times$ ein Erzeuger von $(K^\times, \cdot)$, hat a die Ordnung $q-1$ und $K^\times$ besteht gerade aus den Elementen $1, a, \ldots, a^{q-2}$. Für $a^n \in K^\times$ gilt $(a^n)^{q-1} = (a^{q-1})^n = 1$, daher gilt $k^{q-1} - 1 = 0$ für alle von 0 verschiedenen Elemente k von K und $k^q - k = 0$ für alle $k \in K$ (einschließlich der 0). □

Beispiel 8. Ist p eine Primzahl, existiert ein $a \in \mathbb{F}_p^\times$, so dass $1, a, \ldots, a^{p-2}$ gerade die von Null verschiedenen Elemente in $\mathbb{F}_p$ sind. Ein solches Element a nennt man Primitivwurzel modulo p. Zum Beispiel ist 3 eine Primitivwurzel modulo 7, denn $\{1, 3, 3^2, 3^3, 3^4, 3^5\} = \{1, 3, 2, 6, 4, 5\} = \mathbb{F}_7^\times$.

Satz 9. *$K \subset L$ endlicher Körper, $\alpha_1, \ldots, \alpha_k \in L$ algebraisch über K. Dann gilt $K(\alpha_1, \ldots, \alpha_k) = K(\alpha)$ für ein geeignetes $\alpha \in K(\alpha_1, \ldots, \alpha_k)$.*

Beweis. $K(\alpha_1, \ldots, \alpha_k)$ ist eine endliche Erweiterung von K und somit auch ein endlicher Körper. Nach Satz 6 ist daher die multiplikative Gruppe von $K(\alpha_1, \ldots, \alpha_k)$ zyklisch. Ist α ein erzeugendes Element, gilt $K(\alpha) = K(\alpha_1, \ldots, \alpha_k)$. □

Folgerung 10. *K endlicher Körper der Charakteristik p, $[K : \mathbb{F}_p] = n$. Dann existiert ein $\alpha \in K$, so dass α algebraisch vom Grad n über $\mathbb{F}_p$ ist und $K = \mathbb{F}_p(\alpha)$ gilt.*

Beweis. Die Behauptung folgt direkt aus Satz 9. □

Satz 11.

(a) Jeder endliche Körper hat die Ordnung p^n für eine Primzahl p und eine natürliche Zahl n.

(b) Für jede Primzahl p und jedes $n \in \mathbb{N}$ existiert ein Körper der Ordnung p^n.

(c) Jeder Körper der Ordnung p^n ist (isomorph zum) Zerfällungskörper von $X^{p^n} - X \in \mathbb{F}_p[X]$.

(d) Haben zwei Körper die Ordnung p^n, so sind sie isomorph.

Beweis. (a) folgt aus Satz 1, in dem gezeigt wurde, dass ein endlicher Körper mit Charakteristik p genau p^n Elemente besitzt, wobei n die Dimension des Körpers über $\mathbb{F}_p$ ist.

Sei nun $f = X^{p^n} - X$, L der Zerfällungskörper von f über $\mathbb{F}_p$ und $\alpha \in L$ eine Nullstelle von f. Wir können dann f schreiben als $f = (X - \alpha)^k g \in L[X]$ mit $k \in \mathbb{N}$, $g \in L[X]$, wobei α keine Nullstelle von g ist. Dann ist $f' = -1$ durch $(X - \alpha)^{k-1}$ in $L[X]$ teilbar, woraus $k - 1 = 0$ folgt. Somit ist α einfache Nullstelle von f. Alle Nullstellen von f sind verschieden und f besitzt genau p^n Nullstellen in L. Nun kann man nachrechnen, dass die Produkte, Summen und Inverse der Nullstellen von f wieder Nullstellen von f bilden. Die Nullstellen von f bilden also einen Körper mit genau p^n Elementen. Dieser ist somit der Zerfällungskörper L von f über $\mathbb{F}_p$ und es gilt $[L : \mathbb{F}_p] = n$. Damit sind die Aussagen (b) und (c) bewiesen.

Da Zerfällungskörper (bis auf Isomorphie) eindeutig sind, folgt die Eindeutigkeit (bis auf Isomorphie) aus Aussage (d). □

Folgerung 12. *Für jede natürliche Zahl n und Primzahl p gibt es ein irreduzibles Polynom vom Grad n in $\mathbb{F}_p[X]$.*

Beweis. Nach Satz 11 existiert ein Körper K mit $[K : \mathbb{F}_p] = n$. In diesem Körper existiert nach Folgerung 10 ein $\alpha \in K$, das algebraisch vom Grad n über $\mathbb{F}_p$ ist. Dann ist das Minimalpolynom f von α irreduzibel vom Grad n über $\mathbb{F}_p$ und es ist $K = \mathbb{F}_p(\alpha) \cong \mathbb{F}_p[X]/(f)$. □

Bemerkung 13. Wegen der Eindeutigkeit (bis auf Isomorphie) können wir von *dem* Körper mit p^n Elementen sprechen. Er wird mit $\mathbb{F}_{p^n}$ bezeichnet. Der Primkörper von $\mathbb{F}_{p^n}$ ist isomorph zu $\mathbb{F}_p$.

Die bisherigen Ergebnisse gestatten die explizite Konstruktion von endlichen Körpern. Wir wissen, dass $\mathbb{F}_{p^n}$ ein Vektorraum der Dimension n über seinem Primkörper $\mathbb{F}_p$ ist. Weiter gibt es nach Folgerung 10 ein Element $\alpha \in \mathbb{F}_{p^n}$, so dass $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$ ist. Ist $f \in \mathbb{F}_p[X]$ das Minimalpolynom von α, dann gilt $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha) \cong \mathbb{F}_p[X]/(f)$. Wir können also $\mathbb{F}_{p^n}$ konstruieren, indem wir ein irreduzibles, normiertes Polynom f von Grad n über $\mathbb{F}_p$ bestimmen und den Restklassenring $\mathbb{F}_p[X]/(f)$ bilden.

Beispiel 14. Das quadratische Polynom $f = X^2 + X + 1$ ist normiert und irreduzibel über $\mathbb{F}_2$. Der Restklassenring $\mathbb{F}_2[X]/(f)$ ist somit isomorph zu $\mathbb{F}_4$. Wir setzen $\alpha := X + (f) \in \mathbb{F}_2[X]/(f)$, so dass α eine Nullstelle von f in $\mathbb{F}_2[X]/(f)$ ist. Wir können

den Körper $\mathbb{F}_4$ mit $\mathbb{F}_2(\alpha)$ identifizieren. Es ist $(1, \alpha)$ eine Basis von $\mathbb{F}_4$ über $\mathbb{F}_2$. Die Elemente von $\mathbb{F}_4$ sind also gegeben durch $0, 1, \alpha, \alpha+1$. Man rechnet mit diesen Elementen gemäß den Rechenregeln in $\mathbb{F}_2[X]/(f)$. Es ergeben sich die folgenden Verknüpfungstafeln:

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

$\cdot$	1	α	$\alpha+1$
1	1	α	$\alpha+1$
α	α	$\alpha+1$	1
$\alpha+1$	$\alpha+1$	1	α

Wir sehen, dass die multiplikative Gruppe $(\mathbb{F}_4^\times, \cdot)$ von α oder $\alpha+1$ zyklisch erzeugt wird. Es gilt ferner $X^4 - X = X(X-1)(X-\alpha)(X-\alpha-1)$, d. h. die Elemente von $\mathbb{F}_4$ sind gerade die Nullstellen des Polynoms $X^4 - X$ und $\mathbb{F}_4$ ist Zerfällungskörper von $X^4 - X$.

Beispiel 15. Da die Polynome $f = X^2 + 1$ und $g = X^2 + X + 2$ über $\mathbb{F}_3$ irreduzibel sind, erhalten wir mit $\mathbb{F}_3[X]/(f)$ und $\mathbb{F}_3[X]/(g)$ zwei Körper der Ordnung 9. Wegen der Eindeutigkeit des $\mathbb{F}_9$ (bis auf Isomorphie) sind die beiden Körper isomorph. Ist $\alpha = X + (f)$ Nullstelle von f in $\mathbb{F}_3[X]/(f)$ und $\beta = X + (g)$ Nullstelle von g in $\mathbb{F}_3[X]/(g)$, dann definieren wir die $\mathbb{F}_3$-lineare Abbildung $\varphi : \mathbb{F}_3[X]/(f) \to \mathbb{F}_3[X]/(g)$ mit $\varphi(1) = 1$ und $\varphi(\alpha) = 2\beta + 1$. Offensichtlich ist φ ein Isomorphismus von Vektorräumen. Um zu zeigen, dass φ sogar ein Körperisomorphismus ist, müssen wir nachrechnen, dass $\varphi(xy) = \varphi(x)\varphi(y)$ für alle $x, y \in F_3[X]/(f)$ gilt. Seien also $x = a_1\alpha + b_1, y = a_2\alpha + b_2 \in F_3[X]/(f)$ mit $a_1, a_2, b_1, b_2 \in \mathbb{F}_3$. Dann gilt

$$\begin{aligned}
\varphi(xy) &= \varphi\left((a_1\alpha + b_1)(a_2\alpha + b_2)\right) \\
&= \varphi\left(a_1a_2\alpha^2 + b_1b_2 + (a_1b_2 + a_2b_1)\alpha\right) \\
&= \varphi\left(2a_1a_2 + b_1b_2 + (a_1b_2 + a_2b_1)\alpha\right) \quad (\text{wegen } \alpha^2 = 2) \\
&= 2a_1a_2 + b_1b_2 + (a_1b_2 + a_2b_1)(2\beta + 1) \\
&= 2a_1a_2 + b_1b_2 + a_1b_2 + a_2b_1 + (2a_1b_2 + 2a_2b_1)\beta,
\end{aligned}$$

$$\begin{aligned}
\varphi(x)\varphi(y) &= \varphi(a_1\alpha + b_1)\varphi(a_2\alpha + b_2) \\
&= \left(a_1(2\beta + 1) + b_1\right)\left(a_2(2\beta + 1) + b_2\right) \\
&= a_1a_2(2\beta + 1)^2 + b_1b_2 + (a_1b_2 + a_2b_1)(2\beta + 1) \\
&= a_1a_2(\beta^2 + \beta + 1) + b_1b_2 + a_1b_2 + a_2b_1 + (2a_1b_2 + 2a_2b_1)\beta \\
&= 2a_1a_2 + b_1b_2 + a_1b_2 + a_2b_1 + (2a_1b_2 + 2a_2b_1)\beta \quad (\text{wegen } \beta^2 + \beta + 1 = 2) \\
&= \varphi(xy).
\end{aligned}$$

Tatsächlich ist φ ein Isomorphismus zwischen $\mathbb{F}_3[X]/(f)$ und $\mathbb{F}_3[X]/(g)$.

Satz 16. *Seien $m, n \in \mathbb{N}$. Dann gilt: $X^m - 1 \mid X^n - 1 \Leftrightarrow m \mid n$.*

Beweis. „$\Leftarrow$“ Gelte $m \mid n$, d. h. $n = km$ für ein $k \in \mathbb{N}$. Dann folgt

$$\frac{X^n - 1}{X^m - 1} = \frac{X^{km} - 1}{X^m - 1} = \frac{(X^m)^k - 1}{X^m - 1} = 1 + X^m + X^{2m} + \cdots + X^{(k-1)m} \in K[X]$$

„⇒“ Sei $n = km + r$ mit $k, r \in \mathbb{N}$, $0 \leq r < m$ und gelte $X^m - 1 \mid X^n - 1$. Wegen $X^n - 1 = X^{km+r} - 1 = (X^{km} - 1)X^r + (X^r - 1)$ folgt dann $X^m - 1 \mid X^r - 1$ und somit $r = 0$ wegen $0 \leq r < m$. □

Satz 17. *Sei p prim und m,n* $\in \mathbb{N}$. *Dann gilt:*

(a) $\mathbb{F}_{p^m} \leq \mathbb{F}_{p^n} \Rightarrow m \mid n$.

(b) $m \mid n \Rightarrow \mathbb{F}_{p^m} \hookrightarrow \mathbb{F}_{p^n}$.

Beweis. (a) Nach Satz 1.25 (Gradsatz) gilt:

$$[\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}][\mathbb{F}_{p^m} : \mathbb{F}_p].$$

Wegen $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$ und $[\mathbb{F}_{p^m} : \mathbb{F}_p] = m$ folgt direkt $m \mid n$.

(b) Gegeben: $m \mid n$; zu zeigen: $\mathbb{F}_{p^m} \hookrightarrow \mathbb{F}_{p^n}$.
Aus $m \mid n$ erhalten wir durch zweimalige Anwendung von Satz 16 $p^m - 1 \mid p^n - 1$ und $X^{p^m-1} - 1 \mid X^{p^n-1} - 1$
$\Rightarrow X^{p^m} - X \mid X^{p^n} - X$.
Die Nullstellen des Polynoms $X^{p^m} - X$ bilden daher einen Unterkörper U von $\mathbb{F}_{p^n}$. U hat nach Konstruktion p^m Elemente und ist daher zu $\mathbb{F}_{p^m}$ isomorph $\Rightarrow \mathbb{F}_{p^m} \hookrightarrow \mathbb{F}_{p^n}$. □

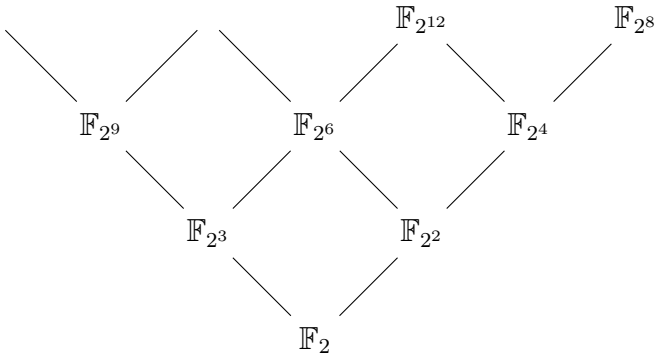


Abbildung 1: Beispiele für Körpereinbettungen

Der obige Satz lässt uns ein sehr anschauliches Beispiel über den Zusammenhang der endlichen Körper erstellen (siehe Abbildung 1). Auf dem Weg nach rechts oben multipliziert man die Potenz mit 2, auf dem Weg nach links mit 3. Die Körper, die sich direkt unter einem Körper befinden, lassen sich in diesen einbetten. In der obigen Additionstabelle des $\mathbb{F}_4$ sieht man ebenfalls, dass sich $\mathbb{F}_2$ in diesen einbetten lässt.

Definition 18. K Körper, $n \in \mathbb{N}$. Ist $\alpha \in K$ eine Nullstelle des Polynoms $X^n - 1 \in K[X]$, so heißt α *n-te Einheitswurzel*. Die Menge der n-ten Einheitswurzeln in K bezeichnen wir mit $\mu_n(K) = \{\zeta \in K : \zeta^n = 1\}$.

Bemerkung 19. K Körper, $n \in \mathbb{N}$. Dann ist $\mu_n(K)$ eine zyklische, endliche Untergruppe von $(K^\times, \cdot)$.

Beweis. Wir rechnen die Untergruppenkriterien nach:

(i) $1 \in \mu_n(K) \Rightarrow \mu_n(K) \neq \emptyset$

(ii) $\alpha^n = \beta^n = 1 \Rightarrow (\alpha\beta)^n = \alpha^n\beta^n = 1$

(iii) $\alpha^n = 1 \Rightarrow (\alpha^{-1})^n = (\alpha^n)^{-1} = 1^{-1} = 1$

Da das Polynom $X^n - 1$ höchstens n Nullstellen besitzt, ist $\mu_n(K)$ endlich. Nach Lemma 6 ist $\mu_n(K)$ zyklisch. □

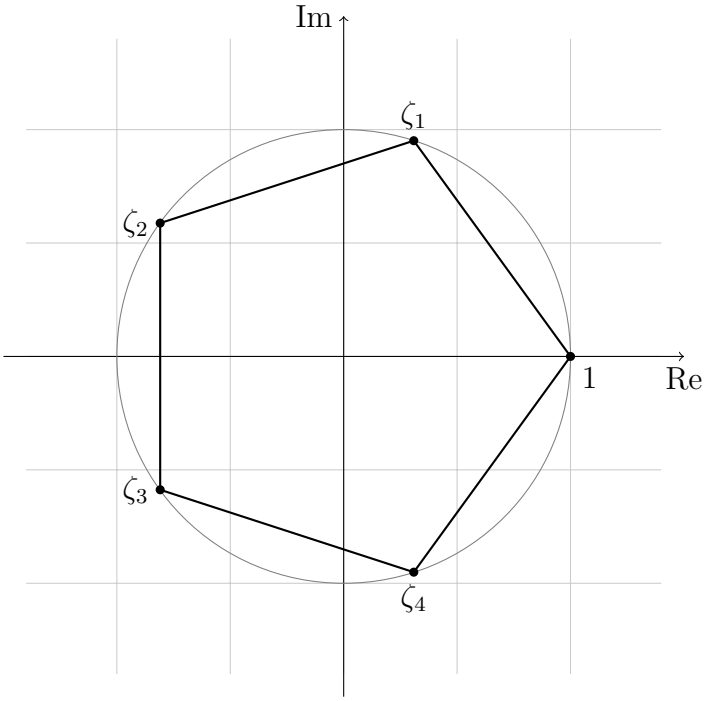
Definition 20. K Körper, $n \in \mathbb{N}$. Hat $\alpha \in \mu_n(K)$ die Ordnung n, heißt α eine *primitive n-te Einheitswurzel*. Der Zerfällungskörper des Polynoms $X^n - 1 \in K[X]$ heißt der *n-te Kreisteilungskörper* oder *zyklotomische Körper* über K.

Beispiel 21. Für $n \in \mathbb{N}$, p prim, $q = p^n$ ist $\mathbb{F}_q$ der $(q-1)$-te Kreisteilungskörper über $\mathbb{F}_p$, da er der Zerfällungskörper des Polynoms $X^{q-1} - 1 \in \mathbb{F}_p[X]$ ist.

Beispiel 22. Für alle $n \in \mathbb{N}$ ist $\mathbb{C}$ selbst der n-te Kreisteilungskörper über $\mathbb{C}$. Die n-ten Einheitswurzeln sind gegeben durch $\zeta_k = e^{2\pi ki/n}$ $(k = 0, 1, \ldots, n-1)$, denn es gilt $\zeta_k^n = e^{2\pi ki} = 1$ und die ζ_k sind paarweise verschieden. Es gilt also

$$X^n - 1 = (X-1)(X - e^{2\pi i/n}) \cdots (X - e^{2\pi i(k-1)/n}).$$

Außerdem gilt $\zeta_1^k = \zeta_k$, also ist $\zeta_1 = e^{2\pi i/n}$ eine primitive n-te Einheitswurzel. In der komplexen Zahlenebene stellen die n-ten Einheitswurzeln die Eckpunkte eines regelmäßigen n-Ecks dar, das dem Einheitskreis einbeschrieben ist. Beispiel $n = 5$:



Lemma 23. *K endlicher Körper der Charakteristik p, $n \in \mathbb{N}$ mit $p \nmid n$. Dann ist das Polynom $X^n - 1 \in K[X]$ separabel, d. h. es besitzt in seinem Zerfällungskörper genau n einfache Nullstellen.*

Beweis. Sei $L \supset K$ der Zerfällungskörper von $f = X^n - 1 \in K[X]$ und $\alpha \in L$ eine Nullstelle von f. Wegen $0^n = 0 \neq 1$ gilt $\alpha \neq 0$. Bekanntlich ist α mehrfache Nullstelle von f, genau dann wenn $f'(\alpha) = 0$ gilt. Es ist aber $f'(\alpha) = n\alpha^{n-1} \neq 0$ wegen $p \nmid n$ und $\alpha \neq 0$. □

Satz 24. *K endlicher Körper der Charakteristik p, $n \in N$ mit $p \nmid n$. Dann ist der n-te Kreisteilungskörper über K eine einfache Erweiterung von K.*

Beweis. Sei L der Zerfällungskörper des Polynoms $X^n - 1 \in K[X]$. Nach Bemerkung 19 bilden die Nullstellen von $X^n - 1$ in L eine zyklische Gruppe. Da diese Nullstellen nach Lemma 23 paarweise verschieden sind, hat die Gruppe genau n Elemente. Sei $\alpha \in L$ ein erzeugendes Element, dann hat α die Ordnung n und ist somit eine primitive n-te Einheitswurzel. Da man durch Adjunktion von α alle n-ten Einheitswurzeln erhält, ist $K(\alpha)$ Zerfällungskörper von $X^n - 1$, also gilt $L = K(\alpha)$. □