Profeesor Dr. Jürgen Ritter
Lehrstuhl für Algebra und Zahlentheorie
Institut für Mathematik · Universität Augsburg

Schülerseminar Mathematik 2002 , Kloster Aldersbach, 26.5. – 1.6. 2002

Endliche Körper und Quadratwurzeln

aufgeschrieben von
Christian Kreuzer, Andreas Nickel und Simone Schuierer

1 . Einführung

Diese einwöchentliche Vortragsreihe resultiert aus der Frage, ob die reellen Zahlen tatsächlich ein überzeugendes Koordinatensystem für Beschreibungen von Phänomenen aus der realen Welt sind. Was stört, könnte deren *lineare Unendlichkeit*, auch *Archimedisches Axiom* genannt, sein, nämlich

(∗) *zu jeder reellen Zahl a gibt es eine natürliche Zahl* [1] *n mit $n > a$.*
"Nichts schließt sich."

Im folgenden soll deshalb versucht werden, einen *endlichen* Koordinatenkörper K zu erstellen, der zumindest die gängigen geometrischen Konstruktionen, à la Pythagoras etc., erlaubt; es sollen also etwa die Quadratwurzeln aus den ersten N Zahlen von K gezogen werden können, wobei N beliebig groß vorgegeben sein darf (K wird allerdings von N abhängen).

Wir verwenden durchweg diese Abkürzungen: $\forall$ stehe für "für alle" oder "für jedes" und $\exists$ für "es exisitiert ein". Obige Aussage (∗) kann also auch so mitgeteilt werden $\left[\forall a \in \mathbb{R}\, \exists n \in \mathbb{N} : a < n\right]$.

Definition. *Ein Körper K ist eine Menge mit zwei Verknüpfungen, die i.A. mit $+$ und $\cdot$ bezeichnet werden, und folgenden Rechenregeln genügen*

	$+$	$\cdot$
Abgeschlossenheit	$a+b \in K\ (\forall a,b \in K)$	$a \cdot b \in K\ (\forall a,b \in K)$
Kommutativität	$a+b = b+a\ (\forall a,b \in K)$	$a \cdot b = b \cdot a\ (\forall a,b \in K)$
Assoziativität	$a+(b+c) = (a+b)+c\ (\forall a,b,c \in K)$	$a \cdot (b \cdot c) = (a \cdot b) \cdot c\ (\forall a,b,c \in K)$
Neutrales Element	$\exists 0 \in K : a+0 = a\ (\forall a \in K)$	$\exists 1 \in K : a \cdot 1 = a\ (\forall a \in K)$
Inverses Element	$\forall a \in K\ \exists -a \in K : a+(-a) = 0$	$\forall 0 \neq a \in K\ \exists a^{-1} \in K : a \cdot a^{-1} = 1$
Distributivität	$a \cdot (b+c) = a \cdot b + a \cdot c\ (\forall a,b,c \in K)$.	

[1] das sind die Zahlen $1, 2, 3, \cdots$; ihre Gesamtheit werde mit $\mathbb{N}$ bezeichnet; mit $\mathbb{Z}$ die der ganzen Zahlen $\{\cdots, -3, -2, -1, 0, 1, 2, \cdots\}$ und mit $\mathbb{R}, \mathbb{C}$ die der reellen bzw. komplexen Zahlen

Beispiele: $K_2 = \{0,1\}$ mit $1+1=0$; $K_4 = \{0,1,a,a^2\}$ mit $a^3 = 1$, $1+1=0$, $1+a=a^2$.

Bemerkung: Wir schreiben im folgenden $n \cdot 1$ für $\underbrace{1+1+\ldots+1}_{n-mal}$. Es gilt dann

$$(n \cdot 1) \dot{+} (m \cdot 1) = (n \dot{+} m) \cdot 1 \,.$$

DEFINITION. *Sei K ein endlicher Körper. Dann heiße die durch K bestimmte kleinste natürliche Zahl n mit $n \cdot 1 = 0$ die Charakteristik von K, also*

$$char(K) = min\{m \in \mathbb{N} \text{ mit } m \cdot 1 = 0\} \,.$$

Wegen der Endlichkeit von K existieren solche m. Die Charakteristik ist eine Primzahl, denn

> $n = char(K) = n_1 \cdot n_2$ mit $n_1, n_2 \in \mathbb{N} \Rightarrow n \cdot 1 = (n_1 \cdot 1) \cdot (n_2 \cdot 1) = 0 \Rightarrow n_1 \cdot 1 = 0$ oder $n_2 \cdot 1 = 0$, ein Widerspruch zur Minimalität von n.

Beispiel: Konstruktion eines Körpers mit p Elementen, p eine Primzahl.

$K_p \overset{\text{def}}{=} \{0,1,2,\ldots,p-1\}$ bildet mit $\odot$ und $\oplus$ einen Körper mit p Elementen, wobei wir, für $a,b \in K_p$, $\quad a \oplus b = r$ über $a+b = v \cdot p + r$ $(0 \le r \le p-1)$ definieren und analog $a \odot b = s$ über $a \cdot b = v \cdot p + s$ $(0 \le s \le p-1)$.

Die Addition und Multiplikation enstehen also aus der Division durch p mit Rest.

Die Existenz des multiplikativen Inversen sieht man folgendermaßen. Erst hier geht ein, daß p eine Primzahl ist.
Betrachte für $0 \neq a \in K$ die Menge $M = \{a \odot x \mid x \in K_p\} \subset K_p$. Dann hat M genauso viele Elemente wie K_p, denn

$$a \odot x_1 = a \odot x_2 \Rightarrow a \cdot (x_1 - x_2) = v \cdot p \Rightarrow x_1 \oplus (-x_2) = 0 \Rightarrow x_1 = x_2 \in K_p \,.$$

Daraus folgt der Reihe nach: $K_p = M$, $\quad 1 \in M$, $\quad \exists a^{-1} \in K_p$ mit $a \odot a^{-1} = 1$.

Ab jetzt lassen wir den Kreis um $\cdot$ und $+$ weg.

2. KONSTRUKTION NEUER KÖRPER

Sei K endlicher Körper und $K[x]$ die Gesamtheit der Polynome in einer Unbestimmten x mit Koeffizienten aus K. Ein Element $f(x) \in K[x]$ ist daher von der Form

$$f(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \ldots + a_1 \cdot x + a_0$$

mit $a_i \in K$ $(0 \le i \le n)$ und mit $n \in \mathbb{N}$. Ist $a_n \neq 0$, so heißt n der Grad von $f(x)$.
Gleichheit, $+$ und $\cdot$ sind auf natürliche Weise erklärt.

Beobachtungen:

> Zu $f(x)$ und $g(x) \neq 0$ existieren Polynome $v(x)$ und $r(x)$ in $K[x]$ mit $f(x) = v(x)g(x) + r(x)$, wobei $r(x) = 0$ oder $grad(r(x)) < grad(g(x))$. Anschaulich ist das die Polynomdivision von $f(x)$ durch $g(x)$ mit Rest $r(x)$.
>
> Ist L ein Körper, der K enthält, so können wir die Koeffizienten eines Polynoms $f(x) \in K[x]$ in L lesen und dann für x Elemente $c \in L$ in $f(x)$ einsetzen.

Für $c \in L$ und $f(x) \in K[x]$ gilt: $f(c) = 0 \Leftrightarrow (x - c)$ teilt $f(x)$ in $L[x]$.
Insbesondere hat $f(x)$ höchstens $grad(f(x))$ viele Nullstellen in L.

DEFINITION. *Ein Polynom $0 \neq f(x) \in K[x]$ heiße irreduzibel, falls aus $f(x) = g_1(x) \cdot g_2(x)$ stets $grad(g_1(x)) = 0$ oder $grad(g_2(x)) = 0$ folgt.*

Übung: Welches sind die irreduziblen Polynome vom Grad 2 in $K_4[x]$?

Das Hauptbeispiel eines Erweiterungskörpers:

Die Polynome vom Grad kleiner als $grad(f(x))$, für ein irreduzibles $f(x) \in K[x]$, bilden mit der natürlichen Addition und folgender Multiplikation $\odot$ einen Körper K_f:

$h_1(x) \odot h_2(x) = r(x)$ mit $h_1(x) \cdot h_2(x) = v(x) \cdot f(x) + r(x)$ mit $r(x)$ wie oben.

Zur Existenz eines Inversen zu $h(x) \neq 0$ mit $grad(h(x)) < grad(f(x))$ betrachte die Menge $\{h(x) \odot g(x) \mid grad(g(x)) < grad(f(x))\}$ und schließe wie oben.

Besitzt K genau q Elemente, so zeigen einfache kombinatorische Überlegungen, daß unser neu konstruierter Körper K_f genau $q^{grad(f(x))}$ Elemente enthält. Insbensondere hat jeder endliche Körper K mit Charakteristik p genau p^n Elemente (für ein $n \in \mathbb{N}$). Ist $K \subset L$ für einen endlichen Körper L, so hat L genau p^s Elmente mit $n \mid s$.

Sei nun $K \subset L$ ein Paar endlicher Körper und $c \in L$. Setze

$$C \stackrel{\text{def}}{=} \{\text{Polynome aus } K[x] \text{ mit Nullstelle } c \text{ in } L\}\,.$$

C besteht nicht nur aus dem Nullpolynom, da unter den Elementen $1, c, c^2, \ldots$ in L Gleichheiten wie etwa $c^n = c^m$ für $0 < n < m$ vorkommen; also ist c Nullstelle von $x^m - x^n$.

$f_c(x)$ sei ein normiertes Polynom kleinsten Grades in C. Dieses ist irreduzibel. (Angenommen, $f_c(x) = g_1(x) \cdot g_2(x)$ mit $grad(g_1(x)),\ grad(g_2(x)) > 0$. Aus $g_1(c) = 0$ oder $g_2(c) = 0$ resultiert der Widerspruch zur Minimalität von $f_c(x)$.)
$f(x)$ teilt jedes $h(x) \in C$: $\quad h(x) = v(x) \cdot f_c(x) + r(x) \Rightarrow r(c) = 0 \Rightarrow r(x) = 0$, letzteres wegen der Minimalität von $f_c(x)$.
Insbesondere ist $f_c(x)$ eindeutig durch c bestimmt.

Setze nun $L_c = \{b_0 + b_1 c + \ldots + b_{n-1} c^{n-1} \mid b_i \in K\} \subset L$ mit $n = grad(f_c(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 \cdot x + a_0)$. L_c enthält K und ist unter der Addition und Multiplikation (in L) abgeschlossen (denn $c^n = -a_{n-1}c^{n-1} - \ldots - a_0$, etc.)

Und die Multiplikation mit einem $0 \neq l \in L_c$ führt die endliche Menge L_c in sich über und erreicht jedes Element (denn $l \cdot l_1 \in L_c$ durchläuft L_c; $l \cdot l_1 = l \cdot l_2 \Leftrightarrow l \cdot (l_1 - l_2) = 0 \stackrel{l \neq 0}{\Rightarrow} l_1 - l_2 = 0 \Leftrightarrow l_1 = l_2$), also ist L_c ein Körper.

Wegen der Minimalität von $f_c(x)$ gilt auch:

$$b_0 + b_1 c + \ldots + b_{n-1} c^{n-1} = d_0 + d_1 c + \ldots + d_{n-1} c^{n-1} \Leftrightarrow b_i = d_i \ (\forall 0 \leq i \leq n-1)\,.$$

Insbesondere hat L_c genau q^n Elemente (falls K genau q Elemente besitzt).

Übung: $f(x) \in K[x]$ sei irreduzibel vom Grad ≥ 2. Nenne in $L \stackrel{\text{def}}{=} K_f$ das Element $x = c$ und zeige $\quad f_c(x) = f(x)$ sowie $L_c = K_f$.

SATZ. *Besitzt K genau $q = p^k$ Elemente, so ist K genau die Nullstellenmenge von $x^q - x \in K_p[x]$. Also ist K durch q eindeutig bestimmt.*

Beweis: Sei $0 \neq a \in K$. Wir wissen bereits, daß es Elemente $n < m$, $n, m \in \mathbb{N}$ mit $a^{m-n} = 1$ gibt. Wir bezeichnen mit e das Minimum der Menge $\{s \in \mathbb{N} \mid a^s = 1\}$. Dann sind $1, a, a^2, \ldots, a^{e-1}$ paarweise verschieden. Falls möglich, wählen wir $0 \neq b \in K$ mit $b \neq a^i$ $(0 \leq i \leq e-1)$. Dann sind $b, ba, ba^2, \ldots, ba^{e-1}$ paarweise verschieden und ungleich allen a^i $(0 \leq i \leq e-1)$. Durch Fortsetzen dieses Verfahrens erhalten wir

$$K \setminus \{0\} = \{1, a, a^2, \ldots, a^{e-1}\} \dot\cup \{b, ba, ba^2, \ldots, ba^{e-1}\} \dot\cup \{c, ca, ca^2, \ldots, ca^{e-1}\} \dot\cup \ldots$$

Also ist e ein Teiler von $q-1$. Es folgt: $a^{q-1} = (a^e)^{\frac{q-1}{e}} = 1 \Rightarrow a^q = a$, d.h. a liegt in der Nullstellenmenge von $x^q - x$.

Wir wollen nun umgekehrt zeigen, daß für einen Körper K mit q Elementen und ein gegebenes $n \in \mathbb{N}$ die Nullstellenmenge $\mathfrak{N}$ von $x^{q^n} - x \in K[x]$ wiederum einen Körper bildet. Indem wir für einen irreduziblen Teiler $f_1(x) \in K[x]$ von $x^{q^n} - x$ den Körper K_{f_1}, dann für einen irreduziblen Teiler $f_2(x) \in K_{f_1}[x]$ von $\frac{x^{q^n}-x}{f_1(x)}$ den Körper $(K_{f_1})_{f_2}$ bilden, und das Verfahren immer weiter fortsetzen, erhalten wir schließlich einen endlichen Körper $L \supset K$, der $\mathfrak{N}$ enthält.
Nun sei p die Charakteristik von K und $a, b \in L$. Dann gilt

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1}b + \ldots \binom{p}{p-1} ab^{p-1} + b^p \ .$$

Da p die Zahlen $\binom{p}{i} = \frac{p!}{i!(p-i)!}$ für $1 \leq i \leq n-1$ teilt, resultiert $(a+b)^p = a^p + b^p$ und allgemeiner $(a+b)^{p^k} = a^{p^k} + b^{p^k}$ für $k \geq 1$. Daraus erhält man die Abgeschlossenheit von $\mathfrak{N}$ unter Multiplikation und Addition, denn für y, z aus der Nullstellenmenge gilt $(yz)^{q^n} = y^{q^n} z^{q^n} = yz$ und $(z+y)^{q^n} = z^{q^n} + y^{q^n} = z + y$. Die anderen Bedingungen an einen Körper sind leicht zu überprüfen.

Übung: K habe q Elemente und $f(x) \in K[x]$ sei irreduzibel und normiert, $n \in \mathbb{N}$. Zeigen Sie:

$$f(x) \mid x^{q^n} - x \Leftrightarrow grad(f(x)) \mid n \ .$$

Eine direkte Konsequenz daraus ist

$$x^{q^n} - x = \prod_{d|n} \prod f_{(d)} \, ,$$

wobei das zweite Produkt über alle irreduziblen normierten Polynome von Grad d zu nehmen ist.
Bezeichnen wir mit $A(d)$ die Anzahl dieser Polynome, so ergibt sich also $q^n = \sum_{d|n} d \cdot A(d)$.

Im weiteren benötigen wir folgende Funktion (*Möbiusfunktion*):

$$\mu(m) = \begin{cases} 1 & \text{falls } m = 1 \\ 0 & \text{falls } m \text{ quadratische Teiler besitzt} \\ (-1)^k & \text{falls } m = p_1 \cdot \ldots \cdot p_k \text{ mit Primzahlen } p_i \end{cases}$$

FOLGERUNG. $n \cdot A(n) = \sum_{d|n} \mu(d) \cdot q^{\frac{n}{d}}$ *; insbesondere ist* $A(n) \neq 0$. *Und: zu jeder Primzahlpotenz* p^n *existiert ein Körper mit* p^n *Elementen.*

Übung: Beweisen sie der Reihe nach:

1. $\mu(n_1 \cdot n_2) = \mu(n_1) \cdot \mu(n_2)$, falls $\mathrm{ggT}(n_1, n_2) = 1$
2. Setze $\beta(n) := \sum_{d|n} \mu(d)$. Dann gilt 1. mit β anstelle von μ.
3. $\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{falls } n = 1 \\ 0 & \text{falls } n > 1 \end{cases}$
4. obige Folgerung mit der Anleitung
$\sum_{d|n} \mu(d) q^{\frac{n}{d}} = \sum_{d|n} \mu(d) \sum_{k|\frac{n}{d}} k \cdot A(k) = \sum_{k|n} \sum_{d|\frac{n}{k}} \mu(d) \cdot k \cdot A(k) = \sum_{k|n} k \cdot A(k) \sum_{d|\frac{n}{k}} \mu(d) = n \cdot A(n)$

Ein Einschub:

LEMMA. *Sind* z_1, z_2 *ganze zueinander teilerfremde Zahlen* $\neq 0$ *(oder zueinander teilerfremde Polynome mit Koeffizienten aus einem Körper* K *), so existieren ganze Zahlen (bzw. Polynome)* t_1, t_2 *mit* $t_1 \cdot z_1 + t_2 \cdot z_2 = 1$.

Beweis (ersetze gegebenenfalls $\mathbb{Z}$ durch $K[x]$):

In $\{n \cdot z_1 + m \cdot z_2 : n, m \in \mathbb{Z}\}$ liegen $\pm z_1, \pm z_2$. Sei d die kleinste positive Zahl darin (bzw. das normierte Polynom kleinsten Grades). Division mit Rest zeigt: $d \mid z_1$,$d \mid z_2$, also $d = 1$.

1. Anwendung:

Ist $f(x)$ irreduzibel, so auch prim [2], d.h.: $f(x) \mid g_1(x) \cdot g_2(x) \Rightarrow f(x) \mid g_1(x)$ oder $f(x) \mid g_2(x)$. Denn falls $f(x) \nmid g_1(x)$, sind $f(x)$ und $g_1(x)$ teilerfremd und wir haben eine Gleichung $t_1(x) \cdot f(x) + t_2(x) \cdot g_1(x) = 1$. Diese multipliziert mit $g_2(x)$ hat links den Faktor $f(x)$, weil $f(x) \mid g_1(x) \cdot g_2(x)$, also auch rechts.

2. Anwendung:

Dividiere der Reihe nach mit Rest

$$\begin{aligned} z_1 &= v_2 \cdot z_2 + z_3 \\ z_2 &= v_3 \cdot z_3 + z_4 \\ &\vdots \\ z_{k-1} &= v_k \cdot z_k + z_{k+1} \\ z_k &= v_{k+1} \cdot z_{k+1} \end{aligned}$$

Lies das rückwärts und finde $z_{k+1} \mid z_k$, $z_{k+1} \mid z_{k-1}, \ldots, z_{k+1} \mid z_2$, $z_{k+1} \mid z_1$. Vergiß die letzte Gleichung und arbeite von unten nach oben, um $1 = z_{k+1} = z_{k+1} - v_k \cdot z_k = z_{k-1} - v_k \cdot z_k = z_{k-1} - v_k \cdot (z_{k-2} - v_{k-1} \cdot z_{k-1}) = \ldots = t_1 \cdot z_1 + t_2 \cdot z_2$ zu erhalten.
Ist nun $z_1 = p$ eine Primzahl oder $z_1 = f(x)$ ein irreduzibles Polynom und $1 \leq z_2 \leq p - 1$ bzw. z_2 ein Polynom mit kleinerem Grad als $f(x)$, so gibt es eine Relation $t_1 \cdot z_1 + t_2 \cdot z_2 = 1$ und es gilt mit $t_2 = v \cdot z_1 + r$, daß r das Inverse von z_2 in K_p bzw. K_f ist.

Hiermit ist also ein explizites Verfahren zur Berechnung von z_2^{-1} in K_p bzw. K_f vorgestellt.

[2] Das haben wir für den Nachweis der Körpereigenschaften von K_f tatsächlich schon benutzt!

Erinnerung: K sei ein Körper mit q Elementen und $0 \neq a \in K$. Dann existiert $e_a = min\{s \in \mathbb{N} : a^s = 1\}$ und $e_a \mid q-1$. Wir nützen das wie folgt aus.

Zerlege $q-1$ in zwei teilerfremde Faktoren: $q-1 = z_1 \cdot z_2$. Wie im Hilfssatz haben wir $t_1 \cdot z_1 + t_2 \cdot z_2 = 1$. Es folgt $a^{t_1 \cdot z_1} \cdot a^{t_2 \cdot z_2} = a$. Der Faktor $a_1 = a^{t_2 \cdot z_2}$ erfüllt $a_1^{z_1} = 1$, der andere Faktor, $a_2 = a^{t_1 \cdot z_1}$, erfüllt $a_2^{z_2} = 1$. Also: Jedes $0 \neq a \in K$ ist Produkt von zwei Elementen a_1, a_2 mit $a_1^{z_1} = 1$, $a_2^{z_2} = 1$.

Allgemeiner: Ist $q-1 = \prod_{i=1}^{r} p_i^{b_i}$, so gilt $a = a_1 \cdot \ldots \cdot a_r$, $a_i^{p_i^{b_i}} = 1$. Gäbe es ein i, so daß für alle $0 \neq a \in K$ bereits $a_i^{p_i^{b_i-1}} = 1$ gelten würde, so hätten wir an der i-ten Stelle höchstens $p_i^{b_i-1}$ Möglichkeiten, also insgesamt weniger als $q-1$.

Resultat: Es existiert ein Element $w_i \in$ mit $w_i^{p_i^{b_i}} = 1$, $w_i^{p_i^{b_i-1}} \neq 1$ für $1 \leq i \leq n$. Damit erfüllt $w \stackrel{\text{def}}{=} \prod_{i=1}^{r} w_i$ die Gleichung $w^{q-1} = 1$, jedoch $w^n \neq 1$ für $n \mid q-1$, $n \neq q-1$. Nun gilt $e_w \mid q-1$, $w^{e_w} = 1$. Deshalb ist $e_w = q-1$.

Zusammenfassung: In K gibt es ein erzeugendes Element w, d.h. $K = \{0, 1, w, w^2, \cdots, w^{e_w-1}\}$. Bislang kennt allerdings niemand eine Formel, die erlauben würde, solch ein w für z.B. $K = K_p$ aus p zu berechnen. Wir müssen also ausprobieren. In K_{17} ist 2 kein w, 3 aber schon.

Ein numerisches Beispiel verdeutliche unsere obige Argumentation für die Existenz eines w noch einmal: K_{49}, also $q-1 = 48 = 2^4 \cdot 3$. Nun ist $2^4 = 16 = 5 \cdot 3 + 1$, also $1 = 1 \cdot 16 - 5 \cdot 3$. Sei jetzt $0 \neq a \in K, e_a$ wie oben (insbesondere: $a^n = 1 \Rightarrow e_a \mid n$, denn $n = v \cdot e_a + r, 0 \leq r \leq e_a, a^n = a^{ve_a} \cdot a^r \Rightarrow a^r = 1$).

Erinnerung: $e_a \mid 48$. $a = \underbrace{a^{1 \cdot 16}}_{=:a_2} \cdot \underbrace{a^{-5 \cdot 3}}_{=:a_1}$. Wir wissen: a_2 erfüllt $a_2^3 = 1$, a_1 erfüllt $a_1^{16} = 1$.

Also: $a = a_1 \cdot a_2$ mit $a_1^{16} = 1, a_2^3 = 1$. Es gibt höchstens 16 Elemente in K mit $a_1^{16} = 1$ und höchstens 3 Elemente mit $a_2^3 = 1$. Wäre nun e_{a_1} stets kleiner als 16, also ein echter Teiler von 16, so gäbe es höchstens 8 Elemente mit $a_1^{16} = 1$, und daher höchstens $3 \cdot 8 = 24$ Elemente in K. Da K jedoch genau 48 Elemente $a \neq 0$ besitzt, existieren also genau 16 Elemente a_1 und genau 3 Elemente a_2.

Damit: $\exists 0 \neq w_1 \in K : e_{w_1} = 16, \exists 0 \neq w_2 \in K : e_{w_2} = 3$. Setze nun $w = w_1 \cdot w_2$ und erhalte $e_w = 48$. Es resultiert $K_{49} = \{0, 1, w, \cdots, w^{47}\}$.

FOLGERUNG. *q sei ungerade.*

a. *Die Quadrate in K sind 0 und w^n mit geradem n*

b. *Quadrat · Quadrat = Quadrat*
Nichtquadrat · Nichtquadrat = Quadrat
Nichtquadrat · Quadrat = Nichtquadrat

Vergleiche die Analogie mit $\mathbb{R}$.

c. *$0 \neq a \in K$ sei gegeben, dann gilt:*

$$a^{\frac{q-1}{2}} = 1 \quad \Leftrightarrow a \text{ ist Quadrat}$$
$$a^{\frac{q-1}{2}} = -1 \quad \Leftrightarrow a \text{ ist Nichtquadrat}$$

Dazu schreibe einfach $a = w^n$.

Beispiel: -1 ist Quadrat in K_p (für $p \geq 3$) $\Leftrightarrow$ p ist von der Form $1 + 4 \cdot m$.

3. Anwendung

Im folgenden ist $K = K_p$ mit einer ungeraden Primzahl p, also $K_p = \{0, 1, \ldots, p-1\} = \{0, 1, w, w^2, \ldots, w^{p-2}\}$. Wir lesen $z \in \mathbb{Z}$ in K_p über die Gleichung $z = v \cdot p + r$, $0 \leq r \leq p-1$; also $z = r$ in K_p.

Definition.

$$\left(\frac{z}{p}\right) = \begin{cases} 0 & p \mid z \\ 1 & z \textit{ ist Quadrat in } K_p \\ -1 & z \textit{ ist Nichtquadrat in } K_p \end{cases}$$

(das Legendre-Symbol).

Beobachtungen zur Definition:

$\left(\frac{z_1 \cdot z_2}{p}\right) = \left(\frac{z_1}{p}\right) \cdot \left(\frac{z_2}{p}\right)$ für $z_1, z_2 \in \mathbb{Z}$

$\left(\frac{1}{p}\right) + \left(\frac{2}{p}\right) + \cdots + \left(\frac{p-1}{p}\right) = 0$

$\left(\frac{z_1}{p}\right) = \left(\frac{z_2}{p}\right)$, wenn z_1 und z_2 den gleichen Rest nach Division durch p lassen.

Wähle nun eine zweite Primzahl $q \neq 2, p$. Insbesondere haben wir, wie für p, das Symbol $\left(\frac{z}{q}\right)$.

$g(x) = x^{q-1} + x^{q-2} + \cdots + x + 1 \in K_p[x]$ habe den irreduziblen Faktor $f(x) \in K_p[x]$: nenne $L = (K_p)_f$. Dann hat $f(x)$ eine Nullstelle ζ in L; diese ist auch Nullstelle von $g(x)$ und von $g(x) \cdot (x-1) = x^q - 1$. Offenbar ist $\zeta \neq 1$, weil $g(1) = q \neq 0$ in K_p.

Setze $\tau = \sum\limits_{i=1}^{q-1} \left(\frac{i}{q}\right) \cdot \zeta^i \in L$ (das ist eine sogenannte Gaußsche Summe)

Behauptungen:

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

Beweis von 1. :

$$\tau^2 = \sum_{i,j} \zeta^{i+j} = \sum_{i=1}^{q-1} \left(\sum_{j=1}^{q-1} \left(\frac{i \cdot j}{q}\right) \cdot \zeta^{i+j} \right)$$

Wir betrachten zunächst den Ausdruck in der Klammer. Beachte hierbei, daß $\left(\frac{i}{q}\right)$ und ζ^i nur vom Rest von i nach Division durch q abhängen. Daher kann j durch $i \cdot j$ substituiert werden:

$$\begin{aligned} \sum_{j=1}^{q-1} \left(\frac{i \cdot j}{q}\right) \cdot \zeta^{i+j} &= \sum_{j=1}^{q-1} \left(\frac{i^2 \cdot j}{q}\right) \cdot \zeta^{i \cdot (1+j)} = \sum_{j=1}^{q-1} \left(\frac{j}{q}\right) \cdot \zeta^{i \cdot (1+j)} = \\ &= \left(\frac{-1}{q}\right) + \sum_{j=1}^{q-2} \left(\frac{j}{q}\right) \cdot \zeta^{i \cdot (1+j)} \end{aligned}$$

$$\begin{aligned}\Rightarrow \tau^2 &= \sum_{i=1}^{q-1}\left(\left(\frac{-1}{q}\right)+\sum_{j=1}^{q-2}\left(\frac{j}{q}\right)\zeta^{i\cdot(1+j)}\right) = \\ &= (q-1)\left(\frac{-1}{q}\right)+\sum_{j=1}^{q-2}\left(\frac{j}{q}\right)\underbrace{\left(\sum_{i=1}^{q-1}\zeta^{i\cdot(1+j)}\right)}_{=\zeta+\ldots+\zeta^{q-1}=-1} = \left(\frac{-1}{q}\right)\cdot q\end{aligned}$$

Beweis von 2. :

$$\tau^p = \sum_{i=1}^{q-1}\left(\frac{i}{q}\right)^p\cdot\zeta^{p\cdot i} = \sum_{i=1}^{q-1}\left(\frac{i}{q}\right)\cdot\zeta^{p\cdot i} = \sum_{i=1}^{q-1}\left(\frac{p}{q}\right)\cdot\left(\frac{p\cdot i}{q}\right)\cdot\zeta^{p\cdot i} = \left(\frac{p}{q}\right)\cdot\tau$$

Folgerungen aus den Behauptungen:

Wegen 1. ist $\tau\neq 0$, wegen 2. ist dann $\tau^{p-1}=\left(\frac{p}{q}\right)$.

Also gilt $\left(\frac{p}{q}\right)=\tau^{p-1}=(\tau^2)^{\frac{p-1}{2}}=\left(\frac{-1}{q}\right)^{\frac{p-1}{2}}\cdot q^{\frac{p-1}{2}}$

Die ganz linke und ganz rechte Seite der Gleichung gehören zu K_p, daher

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

denn für $p\nmid z$ ist $\left(\frac{z}{p}\right)=z^{\frac{p-1}{2}}$ in K_p nach der letzten Folgerung in §2.

Wegen

$$\left(\frac{-1}{q}\right)=\begin{cases}1 & \text{falls } q=1+4\cdot m,\ m\in\mathbb{N}\\ -1 & \text{falls } q=3+4\cdot m,\ m\in\mathbb{N}\end{cases}$$

resultiert: Ist p oder q von der Form $1+4\cdot m$ ($m\in\mathbb{N}$), so ist $\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)$.

Läßt jetzt p noch den Rest 1 nach Division durch q, so ist $\left(\frac{q}{p}\right)=1$, also q Quadrat in K_p.

Übung: Die Primzahl p sei von der Form $p=8\cdot m+1$. Beweisen sie gemäß der Anleitung, daß 2 ein Quadrat in K_p ist:

1. Falls $x^2+1\in K[x]$ reduzibel ist, sei $L=K_p$, sonst $L=(K_p)_{x^2+1}$. Sei i eine Nullstelle von x^2+1 in L.

2. In L gilt:
   $(1+i)^2=2\cdot i$
   $(1+i)^{p-1}=(1+i)^{2\cdot\frac{p-1}{2}}=2^{\frac{p-1}{2}}\cdot i^{\frac{p-1}{2}}=2^{\frac{p-1}{2}}$
   $(1+i)=1+i^p=(1+i)^p=(1+i)\cdot(1+i)^{p-1}=(1+i)\cdot 2^{\frac{p-1}{2}}$

3. In K_p gilt $1=2^{\frac{p-1}{2}}$, also ist 2 Quadrat in K_p.

Nun sei N eine große natürliche Zahl (z. B: $N = 10^{1000000}$). Gesetzt, wir wüßten, daß es eine Primzahl p mit $p = v \cdot 8 \cdot N! + 1$ gibt. Dann läßt p nach Division durch 8 (und daher auch durch 4) den Rest 1, also $\left(\frac{2}{p}\right) = 1$ und $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$, $\forall q \neq p$ ungerade. Wir bilden den Körper K_p und wählen irgendeine Zahl z zwischen 1 und N. Dann ist das z Produkt von Primzahlen q. Diese kommen alle in $N!$ als Faktoren vor. Da nun p nach Division durch $N!$ den Rest 1 läßt, ist das auch bei der Division durch q der Fall. Also erhalten wir

$$\left(\frac{z}{p}\right) = \prod_{q|z} \left(\frac{q}{p}\right)^{d_q} = \prod_{2 \neq q|z} \left(\frac{p}{q}\right)^{d_q} \cdot \underbrace{\left(\frac{2}{p}\right)^{d_2}}_{\text{falls } 2|z} = 1$$

da $\left(\frac{2}{p}\right) = 1$ und $p = v \cdot q + 1$.

Damit sind alle natürlichen Zahlen bis N Quadrate in K_p.

Wir müssen nun noch die Existenz einer Primzahl p mit $p = v \cdot 8 \cdot N! + 1$ nachweisen.

Betrachte dazu das reelle Polynom $x^m - 1$ (für ein $m \in \mathbb{N}$). Seine Nullstellen sind die Punkte c mit den Winkeln $j \cdot \frac{2\pi}{m}$,($0 \leq j \leq m-1$) auf dem komplexen Einheitskreis. Für einen Teiler d von m definiere

$$f_d(x) = \prod_{\substack{c^d=1 \\ c^n \neq 1 \ (\forall n: 0<n<d)}} (x - c) \in \mathbb{C}[x]$$

Offenbar ist $f_1(x) = x-1$, und es gilt $x^m - 1 = \prod_{d|m} f_d(x)$. Alle $f_d(x)$ sind tatsächlich normierte ganzzahlige Polynome:

$f_1(x) \in \mathbb{Z}[x]$

für eine Primzahl q ist $f_q(x) = x^{q-1} + \ldots + x + 1 \in \mathbb{Z}[x]$.
(Denn: $x^q - 1 = \underbrace{(x-1)}_{=f_1(x)} \cdot \underbrace{(1 + x + \ldots + x^{q-1})}_{=f_q(x)}$).

Polynomdivision zeigt nun, daß

$f_{q^2}(x) = \frac{x^{q^2}-1}{f_1(x) \cdot f_q(x)} \in \mathbb{Z}[x]$

$f_{q_1 \cdot q_2}(x) = \frac{x_1^{q_1 \cdot q_2}-1}{f_1(x) \cdot f_{q_1}(x) \cdot f_{q_2}(x)} \in \mathbb{Z}[x]$ etc.

Insbesondere gilt $f_d(0) = \pm 1$.

Setze jetzt $m = 8 \cdot N!$. Wähle ein $g \in \mathbb{Z}$ so groß, daß $f_m(x) = \pm 1$ nur Lösungen $< gm$ hat. Dann ist $f_m(gm) \neq 0, \pm 1$ und besitzt somit einen Primteiler p [3]. Wegen $f_m(0) = \pm 1$, teilt p das m nicht: $p \mid f_m(gm) = (gm)^R + b_{R-1} \cdot (gm)^{R-1} + \ldots + gm \pm 1$ mit gewissen $b_i \in \mathbb{Z}$ impliziert nämlich $p \nmid m$.

Nun gilt für einen Teiler $d \neq 1$ von m:

$$(*)\ 1 + x^{\frac{m}{d}} + x^{\frac{2m}{d}} + \ldots + x^{\frac{(d-1)\cdot m}{d}} = \frac{x^m - 1}{x^{\frac{m}{d}} - 1} = f_m(x) \cdot h(x) \text{ mit einem } h(x) \in \mathbb{Z}[x]\,.$$

[3] Da $gm = g8N!$ i.A. sehr groß sein wird, ist es rechnerisch nicht mehr möglich, ein solches p wirklich zu bestimmen.

Es folgt:

$p \mid f_m(gm) \Rightarrow p \mid (gm)^m - 1 \Rightarrow e_{gm} \mid m$ (wobei gm jetzt in K_p zu lesen ist). Wäre $e_{gm} < m$, also ein echter Teiler, dann wäre $(gm)^{\frac{m}{d}} = 1$ für einen Teiler $d \neq 1$ von m und $d = 0$ in K_p (setze hierzu gm in die Gleichung $(*)$ ein und erhalte

$$p \mid f_m(gm) \mid f_m(gm) \cdot h(gm) = 1 + (gm)^{\frac{m}{d}} + (gm)^{\frac{2m}{d}} + \ldots + (gm)^{\frac{(d-1)\cdot m}{d}} = \underbrace{1 + 1 + \ldots + 1}_{d-mal} =$$

$d \Rightarrow p \mid d \Rightarrow d = 0$ in K_p.)

Damit gilt $e_{gm} = m$, und es folgt $m \mid p - 1$, also $p = v \cdot m + 1 = v \cdot 8 \cdot N! + 1$.

Übung: 1. Warum kommen $2, 3, 4, 5$ nicht als w in K_{241} in Frage?

2. Geben Sie einen Körper K_p an, in dem die Ordnungen e_z für $z = 2, 3, 5, 7$ echte Teiler von $p - 1$ sind!

3. Zeigen Sie, daß es unendlich viele Primzahlen p mit $e_2 < p - 1$ gibt.
Anleitung: Sind schon r solche Primahlen $p_1, \ldots, p_r$ gefunden, so setze in $f_8(x) = x^4 + 1$ den Wert $8 \cdot p_1 \cdot \ldots \cdot p_r$ ein.