6.2. Ringe und Körper

Wir betrachten nun Mengen (endlich oder unendlich) mit zwei Operationen. Diese werden meist als Addition und Multiplikation geschrieben. Meist ist dabei die additiv geschriebene Verknüpfung kommutativ.

DEFINITION 6.2.1. Ring

Eine Menge R mit zwei Verknüpfungen (d.h. Abbildungen $R \times R \to R$) $+$ und $\star$ ist ein *Ring* wenn folgende Eigenschaften erfüllt sind:

(1) $+$ ist assoziativ
(2) Es gibt eine 0 für $+$
(3) Es gibt ein negatives Element bezüglich $+$
(4) $+$ ist kommutativ
(5) $\star$ ist assoziativ
(6) $x \star (y + z) = (x \star y) + (x \star z)$ und $(x + y) \star z = (x \star z) + (y \star z)$, d.h. $\star$ ist distributiv über $+$

Diese Bedingungen sagen, dass $(R, +)$ eine Abelsche Gruppe ist.

EXAMPLE 6.2.2. Ringe

Die ganzen Zahlen $\mathbb{Z}$ bilden einen Ring bezüglich der Addition und Multiplikation. Dieser Ring hat die zusätzliche Eigenschaft, dass die Multiplikation kommutativ ist und es bezüglich der Multiplikation eine 1 gibt. Es ist ein kommutativer Ring mit 1. Analog auch $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. Die Quaternionen sind auch ein Ring, aber nicht kommutativ.

Die Menge der geraden ganzen Zahlen (diese werden mit $2\mathbb{Z}$ bezeichnet) bilden einen Ring. Dies ist ein kommutativer Ring ohne 1.

Die Menge der quadratischen Matrizen über $\mathbb{R}$ (oder einem anderen Ring) bilden einen Ring. Es gibt eine 1 der Ring ist aber nicht kommutativ.

Die Menge der Kongruenzklassen $\mathbb{Z}_n$ bei Division durch n. Dieser Ring ist kommutativ mit 1. Einige Klassen sind invertierbar. Dies ist der sog. *Restklassenring*.

Bereits bei den Kongruenzklassen haben wir *Nullteiler* in einem Ring R kennen gelernt. Dies waren $x, y \in R$ verschieden von 0 mit der Eigenschaft $xy = 0$. Auch der Matrizenring hat Nullteiler:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Eine weitere wichtige Beispielklasse sind die Polynome mit Koeffizienten wieder aus einem Ring R. (Multiplikation und Addition von Polynomen sollte bekannt sein) Die Menge der Polynome über R wird mit $R[x]$ bezeichnet, wobei x die verwendete Variable ist. Ist R kommutativ, dann ist auch $R[x]$ kommutativ, hat R eine 1,dann hat auch $R[x]$eine 1.

Ähnlich ist auch die Defintion von $\mathbb{Z}[\sqrt{2}] := \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$. Auch das ist ein Ring, er ist kommutativ mit 1.

Die Null spielt eine besondere Rolle in einem Ring, denn man hat

LEMMA 6.2.3. *Multiplikation mit Null*

Sei R ein Ring und $x \in R$, dann hat man:

$$0x = 0 = x0.$$

BEWEIS. Man hat $0x = (0 + 0)x = 0x + 0x$, nun addiert man auf beiden Seiten das additiv inverse von $0x$ und bekommt

$$0 = 0x - 0x = 0x + 0x - 0x = 0x.$$

Die zweite Hälfte geht analog. □

Der nächste Schritt ist jetzt der Fall, dass die Multiplikation auf $R\backslash 0$ eine Abelsche Gruppe ist:

DEFINITION 6.2.4. Körper

Ein *Körper* ist eine Menge F mit zwei Verknüpfungen $+, \star$ sodass:

F ist ein Ring mit $1 \neq 0$.

$\star$ ist kommutativ

jedes $x \in F\backslash 0$ hat ein inverses bezüglich $\star$

EXAMPLE 6.2.5. Körper

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$

Restklassenring $\mathbb{Z}_p$ falls p eine Primzahl ist. Dies sind Beispiele für endliche Körper.

Schon bei den Kongruenzklassen haben wir gesehen, dass Nullteiler 'störend' sind, denn es gilt ganz allgemein (vgl 2.4.11)

LEMMA 6.2.6.

Nullteiler in einem Ring sind nicht invertierbar.

BEWEIS. Annahme es gibt einen invertierbaren Nullteiler a im Ring R, d.h. es gibt ein $b \neq 0$ mit $ab = 0$. Diese Gleichung wird mit a^{-1} multipliziert und man bekommt $b = 0$. □

Nullteiler sind hinderlich wenn man Ringe sucht, die Körper sein sollen. Körper spielen eine wichtige Rolle bei Vektorräumen. Hier wird der Körper für die Skalarmultiplikation benötigt. Weitere Strukturen mit 3 Verknüpfungen werden meist Algebra genannt. Wir haben dies z.B. bei der Booleschen Algebra kennengelernt.

6.3. Polynome

Bei der allgemeinen Definition von Ringen wurde auf 'zahlentheoretische' Eigenschaften keinerlei Wert gelegt. Das heisst die Frage inwiefern z.B. Dinge wie die eindeutige Zerlegung in Primfaktoren auch bei allgemeineren algebraischen Strukturen gelten. Wir werden dies im Folgenden genauer für Polynome untersuchen. Ein *Polynom* p (in einer Variable x) über dem Ring R kann man formal als eine Folge $(c_0, c_1, \ldots)$ über R definieren, wobei nur endlich viele Folgenglieder verschieden von 0 sind. Die Menge der Polynome (ein Ring) wird mit $R[x]$ bezeichnet. Bei Polynomen haben wir immer die Darstellung $c_0 + c_1 x + c_2 x^2 + \ldots + c_n x^n$ vor Augen, was impliziert dass alle Koeffizienten c_i für $i > n$ gleich 0 sind. Das maximale n mit $c_n \neq 0$ heisst *Grad* des Polynoms und wird mit $deg(p)$ bezeichnet. Das Nullpolynom hat Grad -1. Der zugehörige Koeffizient heisst *Leitkoeffizient* des Polynoms. Polynome vom Grad 0 heissen konstant, Polynome vom Grad 1 heissen linear, Polynome vom Grad 2 heissen quadratisch. Dies erklärt sich durch den Zusammenhang mit der zugehörigen *Einsetzungsabbildung* oder auch *Polynomabbildung*. Dies ist die Abbildung

$$\begin{array}{ccc} K & \rightarrow & K \\ x & \mapsto & p(x) \end{array},$$

die dann eben konstant, .. ist. Der Koeffizientenring R muss dann ein Unterring von K sein. Setzt man einen einzelnen Wert α ein spricht man vom Auswerten des Polynoms an der Stelle α. Eine *Nullstelle* eines Polynoms p ist dann ein Wert α mit $p(\alpha) = 0$. α ist eine Nullstelle über K wenn $\alpha \in K$.

EXAMPLE 6.3.1. Polynome

Das Polynom $p = x^2 + 1$ ist vom Grad 2, also quadratisch. Der Leitkoeffizient ist 1. Das Polynom hat keine Nullstelle über $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ aber über $\mathbb{C}, \mathbb{H}$. Es hat auch eine Nullstelle über $\mathbb{Z}_5$. Denn $p(2) = 4 + 1 = 5 = 0$.

6.3.1. Polynomdivision. Wir lernen als erstes die Division mit Rest für Polynome kennen.

LEMMA 6.3.2. *Polynomgrad bei Division*

Seien s, t zwei Polynome über einen Körper K vom Grad n und m.

$$\begin{aligned} s &= a_0 + a_1 x + \ldots + a_n x^n \\ t &= b_0 + b_1 x + \ldots b_m x^m \end{aligned}$$

Dabei sei $n \geq m$. Dann ist der Grad des Polynoms

$$u = s - \frac{a_n}{b_m} x^{n-m} t$$

echt kleiner als der Grad von s.

BEWEIS. Der Grad von u kann höchstens n sein. Der Faktor $\frac{a_n}{b_m}$ ist aber gerade so gewählt, dass der Koeffizient bei x^n Null wird. □

Die wiederholte Anwendung dieses Schrittes ist die Vorgehensweise bei der Polynomdivision. Dabei möchte man ein Polynom f vom Grad n dividieren durch ein Polynom g vom Grad $m < n$. D.h. man möchte bekommen wie bei der Division mit Rest:

$$f = qg + r.$$

EXAMPLE 6.3.3. Polynomdivision

Wir starten mit den beiden Polynomen $f = x^4 - 3x^2 + 2x - 4$ und $g = x^2 - 3x + 2$. Beim ersten Schritt ist $s = f$ und $t = g$. Wir bekommen

$$u_1 = s - x^2 t = x^4 - 3x^2 + 2x - 4 - (x^4 - 3x^3 + 2x^2) =$$

$$= 3x^3 - 5x^2 + 2x - 4.$$

Wir haben $f = x^2 g + u_1$. Dabei ist u_1 von echt kleineren Grad als f. Nun wird u_1 weiter zerlegt. Jetzt ist $s = u_1$ und $t = g$. Wir bekommen

$$u_2 = u_1 - 3xt = 3x^3 - 5x^2 + 2x - 4 - (3x^3 - 9x^2 + 6x) =$$

$$= 4x^2 - 4x - 4.$$

Wir haben $f = x^2 g + 3xg + u_2$. Der Grad von u_2 ist jetzt nur noch 2. Wir können noch einen Divisionschritt anbringen und bekommen

$$f = (x^2 + 3x + 4)g + (8x - 12).$$

Dabei erhält man einen Divisionsrest vom Grad $< deg(g)$.

Das dies funktioniert ist Inhalt des folgenden Satzes

THEOREM 6.3.4. *Polynomdivision*

Seien f, g zwei Polynome über einen Körper K vom Grad n und m.Dabei sei $m > 0$.

Dann gibt es Polynome q und r mit

$$f = qg + r$$

und dabei ist $deg(r) < deg(g)$.

BEWEIS. ähnlich der Division mit Rest im Abschnitt über Zahlen. □

In dieser Darstellung ist q der *Quotient* und r der *Divisionsrest*. Ähnlich der Sprechweise bei den Zahlen sagen wir das Polynom f ist durch das Polynom g *teilbar* wenn der Divisionsrest 0 ist. Das Polynom g *teilt* in diesem Fall das Polynom f.

COROLLARY 6.3.5. *Linearfaktoren*

Ein Polynom f hat die Nullstelle α

$\Longleftrightarrow$

f hat den Teiler $(x - \alpha)$.

BEWEIS. " $\Rightarrow$ ": Wir führen die Division mit Rest für das Polynom f und den das Polynom $g := (x - \alpha)$ aus. Betrachtet man nun die beiden identischen Polynome f und $gq + r$ beim Einsetzen der Nullstelle α, so muss $r(\alpha)$ gleich Null sein, und daher ist $r = 0$ da r ja gradmässig kleiner g ist, also ist r eine Konstante. Also ist $r = 0$ und somit teilt $(x - \alpha)$ das Polynom f.

" $\Leftarrow$ ":Wir wissen $f =: (x - \alpha)q$. Setzt man αein so wird der erste Faktor 0 und somit ist auch $f(\alpha) = 0$. □

Nächste Schritt ist die Definition eines ggT bei Polynomen. Die Vorbereitung ist ein Satz äquivalent zu dem entsprechenden Satz für Zahlen (siehe 2.1.4)

THEOREM 6.3.6. *Satz vom ggt für Polynome*

Seien f, g Polynome verschieden vom Nullpolynom. Dann existiert ein Polynom d mit folgenden beiden Eigenschaften

(1) *d teilt f, d teilt g und*
(2) *ist c ein weiterer Teiler von f und g, dann teilt c auch d.*

BEWEIS. Es wird wieder das Wohlordnungsprinzip angewendet. Diesmal spielt der Grad die gleiche Rolle wie der Betrag der Zahl im ursprünglichen Beweis des ggt-Satzes für natürliche Zahlen. Bezeichne mit S die Menge der Polynome vom Grad ≥ 0 der Form

$$fs + gt.$$

Nun betrachtet man die Menge der natürlichen Zahlen, die als Grad von Polynomen in S vorkommen. Nach dem Wohlordnungsprinzip muss es einen kleinsten solchen Grad geben, denn diese Menge ist nicht leer, da z.B. $f1+g0$ drin liegt. Sei nun $d =: fs+gt$ ein Polynom mit minimalen Grad in S. Wir zeigen nun, dass d beide Eigenschaften hat. Dies geht auch analog dem ursprünglichen Beweis.

Beweis von Eigenschaft 2:
Sei c ein gemeinsamer Teiler von f und g, dann existieren g und h, definiert durch $f =: cx$ und $g =: cy$. Damit ist $d = cxs + cyt = c(xs + yt)$ und damit teilt c auch d.

Beweis von Eigenschaft 1:
Wir zeigen dass $d|f$.Dies reicht völlig aus denn f und g sind vertauschbar. Um zu zeigen, dass $d|f$, betrachten wir die Division mit Rest und wollen zeigen, dass der Rest gerade 0 ist. Nach der Division mit Rest haben wir:

$$f = dq + r,$$

wobei $0 \leq deg(r) < deg(d)$. Nun gilt aber für den Rest

$$r = f - dq = f - (fs + gt)q = f(1 - sq) + g(-tq).$$

Also liegt auch r in S, falls es > 0 ist. Da dies aber eine Verletzung der Minimalität des Grades von d wäre, folgern wir, dass $r = 0$, und somit ist d ein Teiler von f. □

Dieses Polynom d ist ein *grösster gemeinsamer Teiler (ggT)* der Polynome f und g. Der ggT bei Polynomen ist nur bis auf Konstanten eindeutig. Wichtig ist aber wieder, die Charakterisierung als ein Grad-minimales Polynom der Form $d = fs + gt$.

EXAMPLE 6.3.7. ggT bei Polynomen
Betrachte $f = x^4 - 5x^3 + 7x^2 - 5x + 6$ und $g = x^3 - 6x^2 + 11x - 6$. Der erste Schritt ist die Polynomdivision und man bekommt:

$$f = (x + 1)g + (2x^2 - 10x + 12).$$

Der nächste Schritt ist eine zweite Division jetzt mit dem Rest und dem Polynom g :

$$g = (\frac{1}{2}x - \frac{1}{2})(2x^2 - 10x + 12) + 0.$$

Damit ist $2x^2 - 10x + 12$ ein ggT der beiden Polynome f und g. Aber auch das Polynom $x^2 - 5x + 6$ wäre ein ggT. Das Rückwärtseinsetzen liefert dann wie beim ggT der Zahlen die gesuchte Linear (oder Polynom) kombination. In diesem Fall nur ein Schritt und man hat

$$(2x^2 - 10x + 12) = f - (x + 1)g.$$

LEMMA 6.3.8. *verschiedene ggT für Polynome*
Unterschiedliche ggT unterscheiden sich nur durch Multiplikation von Konstanten.

BEWEIS. nach Definition haben vers. ggT gleichen Grad und teilen sich gegenseitig, also unterscheiden sie sich nur durch die Multiplikation mit einer Konstanten. Denn die Multiplikation von Polynomen führt zur Addition des Grades. □

Um den euklidschen Algorithmus für Polynome anzuwenden benötigen wir wie schon im Kapitel über Zahlen folgendes kleines Lemma:

LEMMA 6.3.9. *ggT und Polynomdivision*
Seien f, g Polynome vom Grad ≥ 0. Sei

$$f = gq + r$$

mit $deg(r) > 0$. Dann sind $ggT(f, g)$ und $ggT(g, r)$ bis auf Multiplikation mit Konstanten identisch.

BEWEIS. Wir zeigen wie im Falle der Zahlen, dass beide ggTs Teiler von einander sind und den gleichen Grad haben. Dann unterscheiden sie sich aber nur durch die Multiplikation mit einer Konstanten.Sei d ein ggT von f und g und e sei ein ggT von g und r.
Teil 1: da d sowohl f als auch g teilt, teilt d auch $f - gq$ was r ist. Damit ist d auch Teiler von g und r, daher teilt d denn ggT e. Damit ist auch $deg(d) \leq deg(e)$.
Teil 2: da e sowohl g als auch r teilt, teilt e auch $gq + r$ was f ist. Damit ist e auch Teiler von g und f, daher teilt e denn ggT d. Damit ist auch $deg(e) \leq deg(f)$. □

THEOREM 6.3.10. *Euklidischer Algorithmus für Polynome*
Seien f, g Polynome. Falls f Teiler von g ist, ist $ggT(f, g) = f$. Ansonsten liefert die iterierte Anwendung der Polynomdivision mit Rest eine Folge $r_1, r_2, \ldots, r_n$ von Polynomen mit

$$\begin{array}{rcll} g & = & fq_1 + r_1 & (0 < deg(r_1) < deg(f)) \\ f & = & r_1q_2 + r_2 & (0 < deg(r_2) < deg(r_1)) \\ & \vdots & & \\ r_{n-2} & = & r_{n-1}q_n + r_n & (0 < deg(r_n) < deg(r_{n-1})) \\ r_{n-1} & = & r_nq_{n+1} & \end{array}$$

Dann ist r_n ein ggT von f und g.

BEWEIS. Dies ist nichts anderes als die iterierte Anwendung von 6.3.2 was die strikt fallende Folge der Grade liefert. Die Kette zeigt ferner, dass r_n sowohl g als auch f teilt. □

Auch der erweiterte Euklidsche Algorithmus für Polynome kann über das Matrix verfahren erledigt werden. Dies geschieht analog zum bekannten Verfahren für ganze Zahlen.

EXAMPLE 6.3.11. erweitere Euklid für Polynome mit Matrix

Wir wollen den erweiterten Euklid verwenden um einen ggT der beiden Polynome $f = x^4 + x^3 + x + 1$ und $g = x^3 + x + 1$ zu bestimmen. Als Koeffizientenkörper nehmen wir den Körper mit 2 Elementen = $\mathbb{Z}_2$.Die erste Matrix ist dann

$$\left(\begin{array}{cc|c} 1 & 0 & x^4 + x^3 + x + 1 \\ 0 & 1 & x^3 + x + 1 \end{array}\right).$$

Der erste Schritt ist das Abziehen des $x-$fachen der unteren Zeile von der oberen Zeile. Dabei ist zu beachten, dass in $\mathbb{Z}_2$ gilt $-1 = +1$.

$$\left(\begin{array}{cc|c} 1 & 0 & x^4 + x^3 + x + 1 \\ 0 & 1 & x^3 + x + 1 \end{array}\right) \rightarrow \left(\begin{array}{cc|c} 1 & x & x^3 + x^2 + 1 \\ 0 & 1 & x^3 + x + 1 \end{array}\right)$$

Beim nächsten Schritt kann man entweder von der oberen Zeile die untere abziehen oder aber auch von der unteren die obere, da in beiden Zeilen der gleiche Grad vorliegt. Wir zeihen von der oberen die untere Zeile ab:

$$\left(\begin{array}{cc|c} 1 & x & x^3 + x^2 + 1 \\ 0 & 1 & x^3 + x + 1 \end{array}\right) \rightarrow \left(\begin{array}{cc|c} 1 & x+1 & x^2 + x \\ 0 & 1 & x^3 + x + 1 \end{array}\right).$$

Der nächste Schritt ist das $x-$fache der ersten Zeile von der zweiten abziehen:

$$\left(\begin{array}{cc|c} 1 & x+1 & x^2 + x \\ 0 & 1 & x^3 + x + 1 \end{array}\right) \rightarrow \left(\begin{array}{cc|c} 1 & x+1 & x^2 + x \\ x & x^2 + x + 1 & x^2 + x + 1 \end{array}\right).$$

Im letzten Schritt ziehen wir von der zweiten Zeile die erste ab:

$$\left(\begin{array}{cc|c} 1 & x+1 & x^2 + x \\ x & x^2 + x + 1 & x^2 + x + 1 \end{array}\right) \rightarrow \left(\begin{array}{cc|c} 1 & x+1 & x^2 + x \\ x+1 & x^2 & 1 \end{array}\right).$$

Damit hat man als Ergebnis in der unteren Zeile:

$$1 = ggT(x^4+x^3+x+1, x^3+x+1) = (x+1) \times (x^4+x^3+x+1) + (x^2) \times (x^3+x+1).$$

6.4. Endlicher Körper

Im Kapitel über die Zahlen studierten wir nach dem Euklidschen Algorithmus die Kongruenzklassen der Reste bei der Division. Das wichtigste Ergebnis war die Konstruktion von endlichen Körpern in Falle von Resten bei der Division von Primzahlen. Im Falle von Primzahlen gab es bei der Multiplikation keine Nullteiler, damit waren alle Reste außer der Null invertierbar und wir erhielten so einen Körper der Ordnung p, wobei p eine Primzahl ist. Diese Konstruktion wird in diesem Abschnitt verallgemeinert zur Konstruktion von Körpern der Ordnung p^k.

DEFINITION 6.4.1. kongruente Polynome

Sei f ein Polynom vom Grad ≥ 1. Zwei Polynome r und s sind *kongruent modulo* f falls $r - s$ durch f teilbar ist.

Kongruent sein ist eine Äquivalenzrelation und die Menge der Polynome die zu einem Polynom r kongruent modulo f sind wird mit $[r]_f$ bezeichnet. $[r]_f$ ist die entsprechende *Kongruenzklasse*. Es gibt wieder einen *Standardrepräsentanten*, dies ist das Polynom vom Grad $< deg(f)$ welches wegen der Polynomdivision existiert. (Bei der Division durch f hat der Rest r die Eigenschaft $deg(r) < deg(f)$).

DEFINITION 6.4.2. Addition und Multiplikation von Kongruenzklassen

Sei f ein Polynom vom Grad ≥ 1. Seien r, s Polynome, dann definiert man Summe und Produkt von Kongruenzklassen:

$$\begin{array}{rcrcl} [r]_f & + & [s]_f & := & [r+s]_f \\ [r]_f & \times & [s]_f & := & [r \times s]_f \end{array}$$

Auch hier taucht wieder das Problem der Wohldefiniertheit auf, und es wird durch das entsprechende Lemma gezeigt:

LEMMA 6.4.3. *Wohldefiniertheit von Summe und Produkt bei Kongruenzklassen.*

Sei f ein Polynom vom Grad ≥ 1 und seien a, b, c, d Polynome. Seien dabei $[a]_f = [c]_f$ und $[b]_f = [d]_f$. Dann gilt:

$$\begin{array}{rcl} [a+b]_f & = & [c+d]_f \\ [a \times b]_f & = & [c \times d]_f \end{array} .$$

EXAMPLE 6.4.4. Polynomkongruenzklassen

(1) Betrachte $f = x^2 + 1$ aus $\mathbb{R}[x]$. Als Standardrepräsentanten kommen dann nur das Nullpolynom, konstante Polynome und lineare Polynome in Frage. Daher taucht dann bei der Addition kein Problem auf, die Addition zweier Standardrepräsentanten liefert wieder einen Standardrepräsentanten. Bei der Multiplikation taucht dann ein Problem auf bei der Multiplikation zweier linearer Polynome. Als Beispiel betrachte die Multiplikation der beiden Polynome $r = x + 1$ und $s = x+2$. Um den Standardrepräsentanten zu bekommen rechnet man wie folgt:

$$[rs] = [x^2 + 3x + 2] = [3x + 1].$$

(2) Betrachte nun $f = x^3 + x + 1$ über $\mathbb{Z}_2$. Im Fall von $\mathbb{Z}_p$ als Koeffizientenkörper gibt es nur endlich viele Kongruenzklassen. Im Fall eines Polynoms f vom Grad k sind dies p^k Klassen. In diesem Beispiel sind dies die Klassen

$$[0], [1], [x], [x+1], [x^2], [x^2+1], [x^2+x], [x^2+x+1].$$

Betrachte nun die Potenzen $[x], [x]^2, [x]^3, \ldots$ und man erhält

$[x]$	$[x]$
$[x]^2$	$[x^2]$
$[x]^3$	$[x+1]$
$[x]^4$	$[x^2+x]$
$[x]^5$	$[x^2+x+1]$
$[x]^6$	$[x^2+1]$
$[x]^7$	$[1]$

Dieses Phänomen, dass alle Kongruenzklassen bei der Berechnung der Potenzen der Klasse $[r]$ durchlaufen werden, hat einen besonderen Namen. $[r]$ ist dann ein *primitives* Element bzw eine primitive Kongruenzklasse. Nächster Schritt ist jetzt die Untersuchung der multiplikativen Struktur der Restklassen verschieden von Null. Dazu noch ein weiteres Beispiel.

(3) Betrachte nun $f = x^2 + 1$ über $\mathbb{Z}_2$. Betrachte die Polynom Kongruenzklasse $[x+1]$. Wir haben $[x+1]^2 = [x^2+1] = [0]$. Für die multiplikative Struktur bedeutet dies, wir haben einen Nullteiler.

Dieses Beispiel wollen wir vermeiden. Das Problem war, dass $(x+1)$ ein Teiler von $(x^2+1) \in \mathbb{Z}_2[x]$ war. Ein Polynom heisst *irreduzibel* wenn es keine Teiler vom Grad ≥ 1 hat. Die irreduziblen Polynome spielen jetzt die Rolle der Primzahlen aus dem Kapitel über die Zahlen. Dazu definieren wir noch das multiplikative inverse Element einer Polynom Kongruenzklasse. Eine Polynom Kongruenzklasse $[r]$ hat ein *inverses* Element falls es eine Klasse $[s]$ gibt mit $[r][s] = [1]$. Im obigen zweiten Beispiel haben wir gesehen, dass alle

nicht Null Kongruenzklassen von einem primitiven Element multiplikativ erzeugt wurden, damit haben in diesem Beispiel alle nicht Null Kongruenzklassen ein inverses Element, wir haben in diesem Fall einen Körper mit 8 Elementen erhalten. Allgemein gilt Folgendes:

LEMMA 6.4.5. *wann gibt es inverse?*
Sei f ein irreduzibles Polynom. Dann hat jede nicht Null Polynom Kongruenzklasse modulo f ein inverses Element.

BEWEIS. Sei $[r]_f \neq [0]_f$. Betrachte nun ein d mit $d = ggT(r, f)$. Da d ein Teiler von f ist und f irreduzibel ist, ist d ein konstantes Polynom. Andrerseits können wir d als Polynomkombination schreiben:

$$d = ur + vf,$$

und diese Gleichung kann durch d dividiert werden, und wir erhalten

$$1 = u_1 r + v_1 f.$$

Betrachtet man nun die Restklassen modulo f bekommt man

$$[1] = [u_1][r].$$

Also ist $[u_1]$ das gesuchte Inverse zu $[r]$. □

Damit habe ich nun ein allgemeines Verfahren um einen Körper mit p^r Elementen zu erhalten. Wir starten mit einem irreduziblen Polynom vom Grad r über dem Körper mit p Elementen. Glücklicher Weise gibt es ein solches immer (Satz den wir nicht beweisen). Dann betrachten wir die Kongruenzklassen und diese bilden einen Körper mit p^r Elementen.

EXAMPLE 6.4.6. Körper mit 9 Elementen
Die Aufgabe besteht aus folgenden Teilen:

a) Finden eines irreduziblen Polynoms

b) Finden der Körperelemente

c) Erstellen der Verknüpfungstabellen

Um alle irreduziblen Polynome vom Grad 2 über $\mathbb{Z}_3$ zu bekommen, bestimmen wir zuerst alle vom Grad 1 :

$x+1$	$x+2$	x
$2x+1$	$2x+2$	$2x$

führen dann alle möglichen Multiplikationen durch um Polynome vom Grad 2 zu bekommen. Die nicht als Produkt entstehen sind die irreduziblen:

x^2+1	x^2+2	x^2	x^2+x+1	x^2+x+2
	$=(x+1)(x+2)$	$=x(x)$	$=(x+2)(x+2)$	
	$=(2x+1)(2x+2)$	$=2x(2x)$	$=(2x+1)(2x+1)$	
$2x^2+1$	$2x^2+2$	$2x^2$	$2x^2+x+1$	$2x^2+x+2$
$=(x+1)(2x+1)$		$=x(2x)$		$=(x+1)(2x+2)$
$=(x+2)(2x+2)$				

x^2+x	x^2+2x+1	x^2+2x+2	x^2+2x
$=x(x+1)$	$=(x+1)(x+1)$		$=x(x+2)$
$=2x(2x+2)$	$=(2x+2)(2x+2)$		$=2x(2x+1)$
$2x^2+x$	$2x^2+2x+1$	$2x^2+2x+2$	$2x^2+2x$
$=x(2x+1)$		$=(x+2)(2x+1)$	$=x(2x+2)$
$=2x(x+2)$			$=2x(x+1)$

Wir finden 6 irreduzible Polynome vom Grad 2 über $\mathbb{Z}_3$. Um einen Körper mit 9 Elementen zu bekommen müssen wir ein irreduzibles auswählen: z.B. x^2+x+2. Nun nehmen wir

die 9 Polynome vom Grad < 2 als Standardrepräsentanten und addieren und multiplizieren modulo dem gewählten irreduziblen Polynom: z.B. bei der Multiplikation

$$2x(2x+2) = x^2 + x$$

und die Reduktion liefert:

$$(x^2 + x) : (x^2 + x + 2) = 1 + 1/(x^2 + x + 2) = 1$$

Oder bei der Addition:

$$(2x + 1) + (x + 2) = 0$$

Um die Multiplikation schneller zu machen kann man auch ein primitives Element verwenden, und x ist immer eins.

x		x
x^2	$x^2 : (x^2 + x + 2)$	$2x + 1$
x^3	$(2x^2 + x) : (x^2 + x + 2)$=2 + $(2x + 2)/(x^2 + x + 2)$	$2x + 2$
x^4	$(2x^2 + 2x) : (x^2 + x + 2)$=2 + $(2)/(x^2 + x + 2)$	2
x^5		$2x$
x^6		$x + 2$
x^7		$x + 1$
x^8		1