ENDLICHE KÖRPER

1. KÖRPER AUS POLYNOMRINGEN

Diese Unterlagen fassen den Inhalt des Kapitels 8, Unterkapitel 4 des Skriptums zusammen, so wie diese Inhalte in der Vorlesung präsentiert wurden.
Wir kennen bereits Körper. Dies sind Ringe in denen man auch dividieren kann. Die einfachsten endlichen Körper erhält man aus den (Restklassen)ringen $\mathbb{Z}_n$, wobei (Satz 7.20) n eine Primzahl sein muss. Die endlichen Körper die wir also bereits kennen haben alle p Elemente, wobei p eine Primzahl sein muss. Tatsächlich gibt es aber noch andere (wesentlich interessantere) endliche Körper. Wir erhalten Sie auf eine ganz analoge Methode, wie wir die Körper $\mathbb{Z}_p$, p eine Primzahl, erhalten haben.
Wir betrachten Polynome über einem Körper $\mathbb{Z}_p$, also den Ring $\mathbb{Z}_p[x]$. $\mathbb{Z}_p[x]$ ist natürlich wieder ein unendlich großer Ring, da die Polynome in $\mathbb{Z}_p[x]$ beliebig hohe Grade haben können. Wir möchten mit Hilfe von $\mathbb{Z}_p[x]$ wieder einen endlichen Ring machen und machen alles gleich wie bei der Konstruktion von $\mathbb{Z}_n$ aus $\mathbb{Z}$.
Wir nehmen ein Polynom $f = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$ aus $\mathbb{Z}_p[x]$. Nun betrachten wir die Menge der Reste R die bei Division eines Polynoms p aus $\mathbb{Z}_p[x]$ durch f entstehen können. Nach Satz 8.6 haben die Reste alle einen kleineren Grad als f. Also gilt $R = \{a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 | a_i \in \mathbb{Z}, i \in \{0,\ldots,n-1\}\}$. Jeder der Koeffizienten a_i bei einem Restpolynom kann theoretisch p Werte von 0 bis $p-1$ (wir betrachten Polynome in $\mathbb{Z}_p$!) annehmen. Also gilt: Es gibt p^n Reste.
Nun definieren wir auf R (genauso wie bei $\mathbb{Z}_n$) neue Rechenoperationen $+_{(p)}$ bzw. $-_{(p)}$und $*_{(p)}$. Seien $r_1, r_2 \in R$. Dann definieren wir: $r_1 +_{(p)} r_2 := (r_1 + r_2)\ mod\ p$, $-_{(p)} r_1 = (-r_1)\ mod\ p$ und $r_1 *_{(p)} r_2 := (r_1 \cdot r_2)\ mod\ p$. $+$, $-$ und $\cdot$ sind dabei die gewöhnlichen Rechenoperationen in $\mathbb{Z}_p[x]$. mod p bedeutet wieder, dass zunächst $+$, $-$ bzw. $\cdot$ berechnet wird und von diesem Ergebnis der Rest r bei Division durch p errechnet wird. r ist dann erst das Endergebnis der Rechnung. Im Anschluss werden wir häufig statt $+_{(p)}$ doch wieder nur $+$ etc. schreiben.
Auf diese Weise entsteht zunächst wieder ein Ring R. Der Ring R wir dann meist mit $\mathbb{Z}_p[x]/(f)$ bezeichnet.
Eigentlich wollen wir ja Körper konstruieren. Sie ahnen es vielleicht schon. Damit $\mathbb{Z}_p[x]/(f)$ ein Körper ist muss (in Analogie zu $\mathbb{Z}_n$) "f so etwas wie eine Primzahl sein". Nun, hier bietet sich an, f als irreduzibles Polynom über $\mathbb{Z}_p[x]$ zu wählen. Tatsächlich wird $\mathbb{Z}_p[x]/(f)$ dann ein Körper (Satz 8.20 - steht explizit im Skriptum und wird in der Vorlesung bewiesen).

2. BEISPIELE

Wir konstruieren einen (den) endlichen Körper mit 4 Elementen. $4 = 2^2$, also wählen wir den Polynomring $\mathbb{Z}_2[x]$ und Rechnen mit Restklassen modulo eines irreduziblen Polynoms p vom Grad 2 über Z_2. Der erste Versuch p als $p = x^2 + 1$ zu wählen schlägt fehl, da $\overline{p}(1) = 0$. Damit ist $x^2 + 1$ nicht irreduzibel über $\mathbb{Z}_2$! Tatsächlich ist $x^2 + 1 = (x+1)(x+1)$ in $\mathbb{Z}_2[x]$. Mit $p = x^2 + x + 1$ funktioniert es aber. Zunächst hat p keine Nullstellen, was notwendig für die Irreduzibilität von

p ist (allerdings nicht hinreichend). Wäre nun x^2+x+1 reduzibel, so müsste es 2 Polynome $x+a$ und $x+b$ in $\mathbb{Z}_2[x]$ geben, so dass $p=(x+a)(x+b)$. Dann hätte p aber die Nullstellen a und b in $\mathbb{Z}_2$. Dies ist nicht der Fall. Wir betrachten also nun, den Ring $K := \mathbb{Z}_2[x]/(p)$, also die Menge aller Reste bei Polynomdivision von Polynomen über $\mathbb{Z}_2[x]$ durch p. Da p Grad 2 hat gilt $K := \{a_0+a_1x | a_0,a_1 \in \mathbb{Z}_2\}$, also $K=\{0,1,x,1+x\}$. Wir addieren nun die Polynome in K wie gewohnt komponentenweise über $\mathbb{Z}_2$. Beim Multiplizieren rechnen wir auch zunächst wie gewohnt in $\mathbb{Z}_2$ allerdings werden dabei zunächst Polynome mit größerem Grad als 1 entstehen. Ist dies der Fall muss man das Ergebnis durch p dividieren und den Rest r dieser Division ermitteln. Also $x*x = x^2 = r \ mod \ p$. Es gilt: $x^2 : (x^2+x+1) = 1$ mit $r = 1+x$ Rest. Daher ist $x*x = 1+x$. Das reicht in diesem Fall auch schon aus, die Multiplikation vollständig zu beschreiben.

$+$	0	1	x	$1+x$
0	0	1	x	$1+x$
1	1	0	$1+x$	x
x	x	$1+x$	0	1
$1+x$	$1+x$	x	1	0

$*$	0	1	x	$1+x$
0	0	0	0	0
1	0	1	x	$1+x$
x	0	x	$x+1$	1
$1+x$	0	$1+x$	1	x

Man kann das ganze natürlich auch anders bezeichnen. wenn man etwa für $x=2$ und $1+x=3$ setzt, dann erhält man:

$+$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$*$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Den Körper der komplexen Zahlen kann man übrigens auch so konstruieren. Wir wählen den Polynomring $\mathbb{R}[x]$ und betrachten die Reste bei Division durch das über $\mathbb{R}$ irreduzible Polynom $p=x^2+1$. Wir erhalten dann $\mathbb{C} = \mathbb{R}[x]/(p) = \{a_0 + a_1x | a_0,a_1 \in \mathbb{R}\}$. Tatsächlich ist $x*x = x^2 = r \ mod \ x^2+1$.
$x^2 : (x^2+1) = 1$ mit Rest -1! Also gilt $x^2 = -1$ (Anstatt x schreibt man dann üblicherweise i).
Wir rechnen ein weiteres Beispiel im Körper $K = \mathbb{Z}_3[x]/(f)$ wobei $f = x^2+x+2$. f erweist sich (mit den gleichen Argumenten wie bei p über $\mathbb{Z}_2$ von vorhin) als irreduzibel. Darum ist K ein Körper. Da f vom Grad 2 ist, gibts genau neun mögliche Reste bei Polynomdivision durch f, also ist $K = \{a_0+a_1x | a_0,a_1 \in \mathbb{Z}_3\}$.

Wir berechnen das Produnkt $(1+2x)*2$ in K. Dies ist einfach, da normale Polynommultiplikation direkt $(2+x) \in K$ ergibt. Wir berechnen das Produnkt $(1+2x)*(2+x)$ in K. $(1+2x)*(2+x) = 2+2x+2x^2$. Das Ergebnis liegt noch nicht in K, also müssen wir den Rest bei Division durch f ermitteln. Man zeigt schnell, dass $(2x^2+2x+2) : (x^2+x+2) = 2$ mit Rest $r = 1$. Also gilt $(1+2x)*(2+x) = 1$.
Dieses Resultat verwenden wir gleich um die Gleichung $(1+2x)*z = 2$ in K zu lösen. Aufpassen, z ist jetzt die Variable, nicht x! x ist eine "Zahl" im Körper. Wir multiplizieren die Gleichung mit $(2+x)$ und erhalten $z = 1*z = (2+x)(1+2x)*z = (2+x)*2 = 1+2x$.