Jörg MEYER, Hameln

Januar 2023

Kleine endliche Körper

Nomenklatur

Ein *Körper* ist eine Menge von Elementen, die die Elemente „0“ und „1“ enthält und bei der Addition, Subtraktion und Multiplikation nicht aus der Menge herausführen. Zudem darf man durch alle von „0“ verschiedenen Elemente dividieren, und das Ergebnis ist immer noch in der Menge. Bekannte Beispiele sind die rationalen Zahlen oder die reellen Zahlen, aber es gibt auch Körper mit nur endlich vielen Elementen.

In der englischsprachigen Literatur heißen die endlichen Körper Galois fields (nach Evariste Galois), so dass die englische Überschrift „Small Galois Fields“ lauten würde.

Teilt man 3 oder 5 ganzzahlig durch 2, bekommt man in beiden Fällen den Rest 1. Man sagt, dass 3 und 5 *kongruent* modulo 2 zueinander sind und schreibt $3 \equiv 5 \pmod 2$. Analog ist $3 \equiv 8 \pmod 5$ und $-2 \equiv 3 \pmod 5$.

Beispiel 1: Reste modulo 2

Die kleinsten Reste beim Teilen durch 2 sind 0 und 1; sie bilden einen Körper mit den folgenden Verknüpfungen; dabei ist etwa $1+1=2 \equiv 0 \pmod 2$.

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

Beispiel 2: Reste modulo 3

Die kleinsten Reste modulo 3 sind 0, 1 und 2; sie bilden ebenfalls einen Körper:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Innerhalb der kleinsten Reste modulo 3 ist zum Beispiel $\frac{1}{2} = 2$, weil $2 \cdot 2 = 4 \equiv 1 \pmod 3$ ist.

Beispiel 3: Restklassen modulo 5

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Zum Beispiel ist $\frac{1}{2}=3$, weil $2\cdot 3=6\equiv 1 \pmod 5$ ist.

Gibt es einen Körper mit 4 Elementen?

Die kleinsten Reste modulo 4 bilden keinen Körper, wie man an der Multiplikationstafel sieht:

.	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

In der zu „2“ gehörigen Zeile gibt es keine „1“, so dass die „2“ keine Inverse hat.

Versuchen wir es mit 0 und 1 (jeweils modulo 2) und einem weiteren Element L. Natürlich muss zu dem Körper auch $L+1$ und ebenso L^2 gehören. Damit hätte man schon 5 Elemente, aber da es nur 4 sein sollen, muss $L^2=0$ oder $L^2=1$ oder $L^2=L$ oder $L^2=L+1$ sein. In den ersten drei Fällen wäre $L=0$ oder $L=1$, also bleibt nur $\boxed{L^2=L+1}$. (Über den reellen Zahlen ist $x^2=x+1$ die Gleichung des Goldenen Schnitts.)

Wir rechnen weiter modulo 2 und stellen fest, dass die aus 0, 1, L und $L^2=L+1$ bestehende Menge tatsächlich einen Körper bildet:

+	0	1	L	L+1
0	0	1	L	L+1
1	1	0	L+1	L
L	L	L+1	0	1
L+1	L+1	L	1	0

·	0	1	L	L+1
0	0	0	0	0
1	0	1	L	L+1
L	0	L	L+1	1
L+1	0	L+1	1	L

Was ist L^3? Es ist $L^3=L\cdot L^2=L\cdot(L+1)=L^2+L=1$; L ist also eine (von 1 verschiedene) 3. Einheitswurzel. (Wegen $L^2+L+1=0$ war das zu erwarten, da die von 1 verschiedene dritte Einheitswurzel w wegen $0=w^3-1=(w-1)\cdot\left(w^2+w+1\right)$ die Gleichung $w^2+w+1=0$ erfüllt.)

Die Multiplikationstafel lässt sich daher auch schreiben als

·	L^0	L^1	L^2
L^0	L^0	L^1	L^2
L^1	L^1	L^2	L^0
L^2	L^2	L^0	L^1

Man sieht, dass man auch mit $M:=L^2$ als zusätzlichem Element zu 0 und 1 hätte rechnen können, denn es ist $M^2=L^4=L$ und $M+1=L^2+1=L$.

Man sieht noch etwas mehr: Schreibt man $0=\begin{pmatrix}0\\0\end{pmatrix}$, $1=\begin{pmatrix}1\\0\end{pmatrix}$, $L=\begin{pmatrix}0\\1\end{pmatrix}$, $L^2=1+L=\begin{pmatrix}1\\1\end{pmatrix}$, so findet man

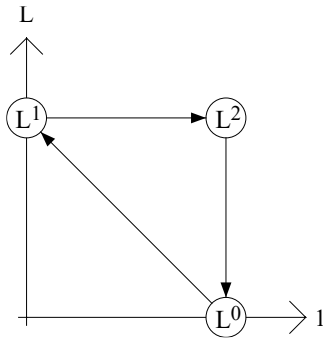
$+$	$\begin{pmatrix}0\\0\end{pmatrix}$	$\begin{pmatrix}1\\0\end{pmatrix}$	$\begin{pmatrix}0\\1\end{pmatrix}$	$\begin{pmatrix}1\\1\end{pmatrix}$
$\begin{pmatrix}0\\0\end{pmatrix}$	$\begin{pmatrix}0\\0\end{pmatrix}$	$\begin{pmatrix}1\\0\end{pmatrix}$	$\begin{pmatrix}0\\1\end{pmatrix}$	$\begin{pmatrix}1\\1\end{pmatrix}$
$\begin{pmatrix}1\\0\end{pmatrix}$	$\begin{pmatrix}1\\0\end{pmatrix}$	$\begin{pmatrix}0\\0\end{pmatrix}$	$\begin{pmatrix}1\\1\end{pmatrix}$	$\begin{pmatrix}0\\1\end{pmatrix}$
$\begin{pmatrix}0\\1\end{pmatrix}$	$\begin{pmatrix}0\\1\end{pmatrix}$	$\begin{pmatrix}1\\1\end{pmatrix}$	$\begin{pmatrix}0\\0\end{pmatrix}$	$\begin{pmatrix}1\\0\end{pmatrix}$
$\begin{pmatrix}1\\1\end{pmatrix}$	$\begin{pmatrix}1\\1\end{pmatrix}$	$\begin{pmatrix}0\\1\end{pmatrix}$	$\begin{pmatrix}1\\0\end{pmatrix}$	$\begin{pmatrix}0\\0\end{pmatrix}$

$\cdot$	$\begin{pmatrix}1\\0\end{pmatrix}$	$\begin{pmatrix}0\\1\end{pmatrix}$	$\begin{pmatrix}1\\1\end{pmatrix}$
$\begin{pmatrix}1\\0\end{pmatrix}$	$\begin{pmatrix}1\\0\end{pmatrix}$	$\begin{pmatrix}0\\1\end{pmatrix}$	$\begin{pmatrix}1\\1\end{pmatrix}$
$\begin{pmatrix}0\\1\end{pmatrix}$	$\begin{pmatrix}0\\1\end{pmatrix}$	$\begin{pmatrix}1\\1\end{pmatrix}$	$\begin{pmatrix}1\\0\end{pmatrix}$
$\begin{pmatrix}1\\1\end{pmatrix}$	$\begin{pmatrix}1\\1\end{pmatrix}$	$\begin{pmatrix}1\\0\end{pmatrix}$	$\begin{pmatrix}0\\1\end{pmatrix}$

Bei der Additionstafel wird komponentenweise modulo 2 addiert.

Bei der Multiplikationstafel bewirkt die Multiplikation mit $L=\begin{pmatrix}0\\1\end{pmatrix}$ dasselbe wie die Multiplikation mit der Matrix $A=\begin{pmatrix}0&1\\1&1\end{pmatrix}$:

$$L=\begin{pmatrix}0\\1\end{pmatrix}=A\cdot\begin{pmatrix}1\\0\end{pmatrix};\ L^2=\begin{pmatrix}1\\1\end{pmatrix}=A^2\cdot\begin{pmatrix}1\\0\end{pmatrix};\ L^3=\begin{pmatrix}1\\0\end{pmatrix}=A^3\cdot\begin{pmatrix}1\\0\end{pmatrix}.$$



Der Körper mit 9 Elementen

Gehen wir analog vor wie beim Körper mit 4 Elementen! Rechnen wir modulo 3 und fügen L als weiteres Element hinzu, was zu der Additionstafel

$+$	0	1	2	L	L+1	L+2	2·L	2·L+1	2·L+2
0	0	1	2	L	L+1	L+2	2·L	2·L+1	2·L+2
1	1	2	0	L+1	L+2	L	2·L+1	2·L+2	2·L
2	2	0	1	L+2	L	L+1	2·L+2	2·L	2·L+1
L	L	L+1	L+2	2·L	2·L+1	2·L+2	0	1	2
L+1	L+1	L+2	L	2·L+1	2·L+2	2·L	1	2	0
L+2	L+2	L	L+1	2·L+2	2·L	2·L+1	2	0	1
2·L	2·L	2·L+1	2·L+2	0	1	2	L	L+1	L+2
2·L+1	2·L+1	2·L+2	2·L	1	2	0	L+1	L+2	L
2·L+2	2·L+2	2·L	2·L+1	2	0	1	L+2	L	L+1

Anlass gibt. Bei der Multiplikationstafel tritt L^2 auf; der Versuch, L^2 mit $L+1$ gleichzusetzen, wird wiederum erfolgreich sein:

·	1	2	L	L+1	L+2	2·L	2·L+1	2·L+2
1	1	2	L	L+1	L−1	2·L	2·L+1	2·L+2
2	2	1	2·L	2·L+2	2·L+1	L	L+2	L+1
L	L	2·L	L+1	2·L+1	1	2·L+2	2	L+2
L+1	L+1	2·L+2	2·L+1	2	L	L+2	2·L	1
L+2	L+2	2·L+1	1	L	2·L+2	2	L+1	2·L
2·L	2·L	L	2·L+2	L+2	2	L+1	1	2·L+1
2·L+1	2·L+1	L+2	2	2·L	L+1	1	2·L+2	L
2·L+2	2·L+2	L+1	L+2	1	2·L	2·L+1	L	2

Wegen $L^2 = L+1$ ist (immer modulo 3 genommen!) ist

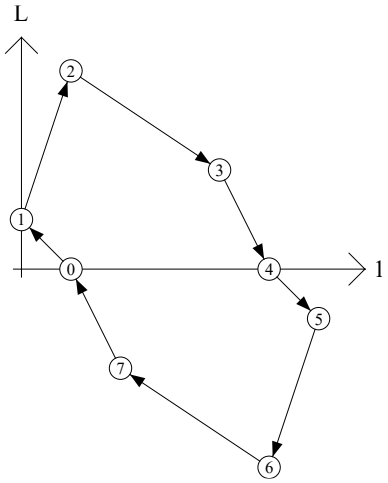
$$1 = L^8;\ 2 = L^4;\ 1+L = L^2;\ 2+L = L^7;\ 2\cdot L = L^5;\ 1+2\cdot L = L^3;\ 2+2\cdot L = L^6 .$$

Damit sind auch hier alle von „0“ verschiedenen Elemente Potenzen von L.

Statt mit L hätte man auch mit L^3 oder L^5 oder L^7 als Basis nehmen können.

Wieder gilt mit $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ die Beziehung $\boxed{L^k = A^k \cdot L^0}$.

Rechts sind nur die Exponenten eingetragen.



Der Körper mit 25 Elementen

Hier kann man nicht $L^2 = L+1$ setzen, da wegen $L^2 - L - 1 \equiv (L-3)^2 \pmod 5$ dann $L = 3$ sein muss.

Besser geht es etwa mit $\boxed{L^2 = 2\cdot L+2}$; nun ist L Basis aller von „0“ verschiedenen Elemente:

	$1 = L^{24}$	$2 = L^{18}$	$3 = L^6$	$4 = L^{12}$
$L = L^1$	$1+L = L^8$	$2+L = L^4$	$3+L = L^{17}$	$4+L = L^3$
$2\cdot L = L^{19}$	$1+2\cdot L = L^{11}$	$2+2\cdot L = L^2$	$3+2\cdot L = L^{21}$	$4+2\cdot L = L^{22}$
$3\cdot L = L^7$	$1+3\cdot L = L^{10}$	$2+3\cdot L = L^9$	$3+3\cdot L = L^{14}$	$4+3\cdot L = L^{23}$
$4\cdot L = L^{13}$	$1+4\cdot L = L^{15}$	$2+4\cdot L = L^5$	$3+4\cdot L = L^{16}$	$4+4\cdot L = L^{20}$

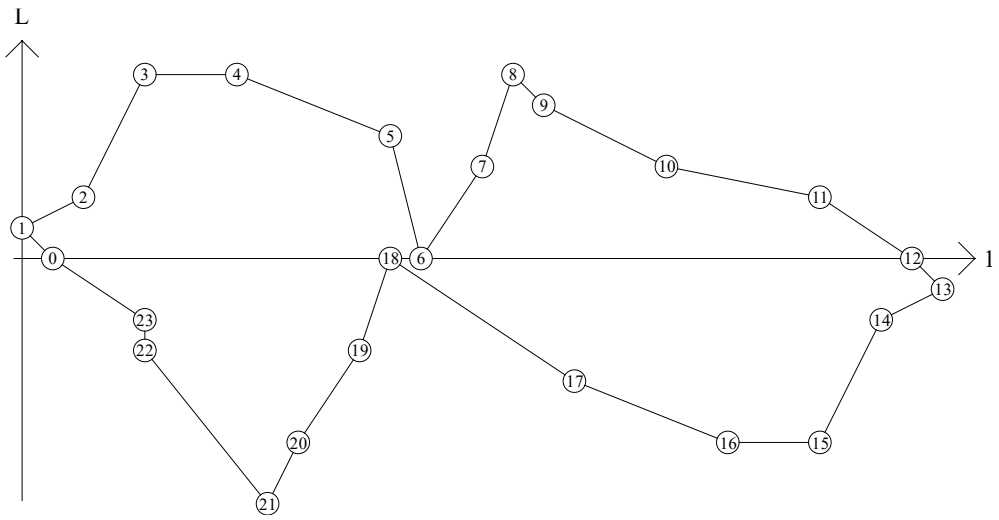
Die Rechnungen kann man dem CAS Maxima überlassen.

```
algebraic:true$

modulus:5$

rat(8);
−2

remainder(L^23, L^2−2·L−2);
−2 L − 1
```



Der Körper mit 8 Elementen

Wir rechnen modulo 2 und fügen zu den Elementen 0 und 1 das Element L hinzu; hier gilt nicht mehr die Gleichung $L^2 = L + 1$. Dann muss es auch die Elemente $1+L$, L^2, $1+L^2$ sowie $L+L^2$ und $1+L+L^2$ geben, was zur (mit einem CAS erstellten) Additionstafel

$$\begin{bmatrix}
0 & 1 & L & 1+L & L^2 & 1+L^2 & L+L^2 & 1+L+L^2 \\
1 & 0 & 1+L & L & 1+L^2 & L^2 & 1+L+L^2 & L+L^2 \\
L & 1+L & 0 & 1 & L+L^2 & 1+L+L^2 & L^2 & 1+L^2 \\
1+L & L & 1 & 0 & 1+L+L^2 & L+L^2 & 1+L^2 & L^2 \\
L^2 & 1+L^2 & L+L^2 & 1+L+L^2 & 0 & 1 & L & 1+L \\
1+L^2 & L^2 & 1+L+L^2 & L+L^2 & 1 & 0 & 1+L & L \\
L+L^2 & 1+L+L^2 & L^2 & 1+L^2 & L & 1+L & 0 & 1 \\
1+L+L^2 & L+L^2 & 1+L^2 & L^2 & 1+L & L & 1 & 0
\end{bmatrix}$$

Im CAS Maxima lautet die Befehlssequenz wie folgt:

```
LL:[0,1,L,1+L,L^2,1+L^2,L+L^2,1+L+L^2];

modulus:2;

algebraic:true;

powerdisp:true;

h[i, k]:=rat(expand(LL[i]+LL[k]));

M1: genmatrix(h, 8, 8);
```

führt. Die (ebenfalls mit einem CAS erstellte) Multiplikationstafel ist komplizierter:

$$\begin{bmatrix} 1 & L & 1+L & L^2 & 1+L^2 & L+L^2 & 1+L+L^2 \\ L & L^2 & L+L^2 & L^3 & L+L^3 & L^2+L^3 & L+L^2+L^3 \\ 1+L & L+L^2 & 1+L^2 & L^2+L^3 & 1+L+L^2+L^3 & L+L^3 & 1+L^3 \\ L^2 & L^3 & L^2+L^3 & L^4 & L^2+L^4 & L^3+L^4 & L^2+L^3+L^4 \\ 1+L^2 & L+L^3 & 1+L+L^2+L^3 & L^2+L^4 & 1+L^4 & L+L^2+L^3+L^4 & 1+L+L^3+L^4 \\ L+L^2 & L^2+L^3 & L+L^3 & L^3+L^4 & L+L^2+L^3+L^4 & L^2+L^4 & L+L^4 \\ 1+L+L^2 & L+L^2+L^3 & 1+L^3 & L^2+L^3+L^4 & 1+L+L^3+L^4 & L+L^4 & 1+L^2+L^4 \end{bmatrix}$$

Nun braucht man in jeder Zeile eine „1“. Der Versuch mit $\boxed{L^3 = 1+L}$ wird erfolgreich sein:

$$\begin{bmatrix} 1 & L & 1+L & L^2 & 1+L^2 & L+L^2 & 1+L+L^2 \\ L & L^2 & L+L^2 & 1+L & 1 & 1+L+L^2 & 1+L^2 \\ 1+L & L+L^2 & 1+L^2 & 1+L+L^2 & L^2 & 1 & L \\ L^2 & 1+L & 1+L+L^2 & L+L^2 & L & 1+L^2 & 1 \\ 1+L^2 & 1 & L^2 & L & 1+L+L^2 & 1+L & L+L^2 \\ L+L^2 & 1+L+L^2 & 1 & 1+L^2 & 1+L & L & L^2 \\ 1+L+L^2 & 1+L^2 & L & 1 & L+L^2 & L^2 & 1+L \end{bmatrix}$$

und liefert zusammen mit

$$L^4 = L + L^2$$
$$L^5 = L^2 + L^3 = 1 + L + L^2$$
$$L^6 = L + L^2 + 1 + L = 1 + L^2$$
$$L^7 = L + 1 + L = 1 = L^0$$

die Tafel

$$\begin{bmatrix} L^0 & L & L^3 & L^2 & L^6 & L^4 & L^5 \\ L & L^2 & L^4 & L^3 & L^0 & L^5 & L^6 \\ L^3 & L^4 & L^6 & L^5 & L^2 & L^0 & L \\ L^2 & L^3 & L^5 & L^4 & L & L^6 & L^0 \\ L^6 & L^0 & L^2 & L & L^5 & L^3 & L^4 \\ L^4 & L^5 & L^0 & L^6 & L^3 & L & L^2 \\ L^5 & L^6 & L & L^0 & L^4 & L^2 & L^3 \end{bmatrix}$$

mit der Befehlssequenz

```
LLL:[1,L,1+L,L^2,1+L^2,L+L^2,1+L+L^2];

modulus:2;

algebraic:true;

powerdisp:true;

h[i, k]:=rat(expand(LLL[i]*LLL[k]));

M1: genmatrix(h, 7, 7);

M2:rat(subst(1+L,L^3, M1));

M3:rat(subst(L+L^2,L^4, M2));

M4:subst(L^3,1+L, M3);

M5:subst(L^4, L+L^2, M4);

M6:subst(L^5, 1+L+L^2, M5);

M7:subst(L^6, 1+L^2, M6);

simp:false;

M8:subst(L^0,1,M7);
```

Hier sind wieder alle Elemente Potenzen von L. Ferner hat man mit der aus 1, L und L^2 bestehenden „Basis“ die Darstellung der von „0“ verschiedenen Elemente

$$\begin{pmatrix}1\\0\\0\end{pmatrix}=L^7,\ \begin{pmatrix}0\\1\\0\end{pmatrix}=L;\ \begin{pmatrix}0\\0\\1\end{pmatrix}=L^2,\ \begin{pmatrix}1\\1\\0\end{pmatrix}=L^3,\ \begin{pmatrix}1\\0\\1\end{pmatrix}=L^6;\ \begin{pmatrix}0\\1\\1\end{pmatrix}=L^4;\ \begin{pmatrix}1\\1\\1\end{pmatrix}=L^5$$

Mit $A=\begin{pmatrix}0&0&1\\1&0&1\\0&1&0\end{pmatrix}$ ist $\boxed{L^k=A^k\cdot L^0}$.

Schlussbemerkung

Wir haben quadratische Körper mit 4 und 9 und 25 Elementen konstruiert und einen kubischen Körper mit 8 Elementen. Man kann beweisen, dass es zu jeder Primzahlpotenz (und *nur* zu einer Primzahlpotenz) einen zugehörigen Körper gibt, und dass dieser Körper (bis auf Umbenennung) eindeutig ist. Die multiplikative Gruppe eines endlichen Körpers wird stets von nur einem Element erzeugt.