Kapitel 2

Gruppen, Ringe und Körper

In diesem Kapitel wollen wir die Rechenregeln, die wir gerade kennengelernt haben, abstrahieren und damit neue algebraische Strukturen definieren. Bevor wir einsteigen und den Begriff der Gruppe definieren, wollen wir die historischen Ursprünge kurz ansprechen. Im wesentlichen geht der Begriff der Gruppe auf das Werk von Évariste Galois (25.10.1811-31.5.1832) zurück, der in der Nacht vor einem Duell sein mathematisches Lebenswerk in einem Brief an einen Freund zu Papier brachte, in dem er sich u.a. mit der Lösbarkeit polynomialer Gleichungen höheren Grades beschäftigte.

2.1 Der Begriff der Gruppe

Wir haben im ersten Kapitel ausführlich mit Resten gerechnet. Dabei haben sich folgende Regeln für Addition der Reste gezeigt. Es gibt ein neutrales Element (Rest 0) und zu jedem Rest ein Inverses. Außerdem gelten Assoziativgesetz und Kommutativgesetz.

Definition 2.1.1
Eine Gruppe *ist eine nichtleere Menge G mit einer Addition $+$, die wir als Paar schreiben wollen $(G, +)$, die folgenden Regeln genügt:*

G1 *Es gilt das* Assoziativgesetz, *d.h. für je drei Elemente $g_1, g_2, g_3 \in G$ gilt*

$$(g_1 + g_2) + g_3 = g_1 + (g_2 + g_3).$$

G2 *Es gibt ein* (links-) neutrales Element, *wir schreiben dafür* 0. *Dies bedeutet für jedes* $g \in G$ *gilt*

$$0 + g = g.$$

Linksneutral *heißt hier, daß nur die Addition von links als neutrales Element fungieren muß. (Es kann und wird sich herausstellen, daß jedes linksneutrale Element in einer Gruppe auch rechtsneutral ist, aber das wissen wir noch nicht.)*

G3 *Zu jedem Element gibt es ein* linksinverses Element, *d.h. zu* $g \in G$ *gibt es ein Element* $\bar{g}$ *mit*

$$\bar{g} + g = 0.$$

Für $\bar{g}$ *schreiben wir auch oft* $-g$.
Gilt zusätzlich für $g_1, g_2 \in G$

G4

$$g_1 + g_2 = g_2 + g_1,$$

so heißt die Gruppe kommutativ.

Beispiel 2.1.2
Als erstes Beispiel betrachten wir die Menge $\mathbb{Z}$ mit der üblichen Addition. Die Gruppe ist kommutativ, wir haben uns bereits davon überzeugt.

Ist $q \in \mathbb{Z}$ $q \neq -1, 0, 1$, so ist $\mathbb{Z}/q\mathbb{Z}$ mit der für die Restklassen eingeführten Addition eine kommutative Gruppe.

Wir wollen nun zeigen, daß wir bei unseren Axiomen die Forderung linksneutral und linksinvers durch neutral und invers ersetzen können.

Satz 2.1.3

1. *Das linksneutrale Element ist auch rechtsneutral.*
2. *Ist* $(-x) + x = 0$, *so ist auch* $x + (-x) = 0$.

Beweis. Wir beginnen mit der zweiten Aussage:

$$\begin{aligned} x + (-x) &= x + (0 + (-x)) \text{ da 0 linksneutral} \\ &= x + (((-x) + x) + (-x)) \text{ da } -x \text{ linksinvers zu } x \\ &= x + ((-x) + (x + (-x))) \text{ Assoziativgesetz} \\ &= (x + (-x)) + (x + (-x)) \text{ Assoziativgesetz .} \end{aligned}$$

Addieren wir nun auf beiden Seiten das linksinverse zu $x+(-x)$ ergibt sich

$$\begin{aligned} 0 &= -(x+(-x)) + ((x+(-x)) + (x+(-x))) \\ &= -((x+(-x)) + (x+(-x))) + (x+(-x)) \\ &= 0 + (x+(-x)) = x+(-x). \end{aligned}$$

Wir kommen zur ersten Aussage

$$x + 0 = x + ((-x) + x) = (x + (-x)) + x = 0 + x.$$

Dabei haben wir die schon bewiesene zweite Aussage und die Assoziativität ausgenutzt. □

Beispiel 2.1.4
Es sei $N = \{1, \ldots, n\}$ die Menge die aus den Zahlen $1, 2, \ldots, n$ besteht. Wir betrachten eine Abbildung dieser Menge auf sich, d.h. eine Funktion $f : N \to N$, die jedem Element aus N ein (i.a. anderes) Element aus N zuordnet. Wir verlangen, daß f injektiv und surjektiv ist. Eine solche Abbildung heißt *Permutation*.

Sind f, g zwei solche Permutationen, so können wir diese verknüpfen und eine neue Permutation $h = f \circ g$ definieren. Diese gibt eine Verknüpfung auf der Menge der Permutationen.

Die spezielle Abbildung $I : N \to N$ mit $I(x) = x$ wirkt als neutrales Element, denn es gilt

$$I \circ f = f \circ I$$

für alle Permutationen f. Da jedes f injektiv ist, ist die Umkehrabbildung definiert, wir schreiben f^{-1}, es gilt

$$f \circ f^{-1} = f^{-1} \circ f = I.$$

Man überzeugt sich leicht von der Richtigkeit

$$f \circ (g \circ h) = (f \circ g) \circ h$$

und sieht damit daß die Menge der Permutationen eine Gruppe bildet. Ist diese Gruppe kommutativ? Bevor wir diese Frage beantworten, wollen wir eine spezielle Schreibweise für Permutationen kennenlernen: zunächst schreiben wir die Zahlen

$$1 \quad 2 \quad \cdot \quad \ldots \quad \cdot \quad n-1 \quad n$$

in einer Reihe und dann die Bilder unter der Permutation jeweils darunter, also

$$\begin{pmatrix} 1 & 2 & \cdot & \ldots & \cdot & n-1 & n \\ f(1) & f(2) & \cdot & \ldots & \cdot & f(n-1) & f(n) \end{pmatrix}.$$

Wichtig dabei ist, daß jede Zahl in der unteren Zeile genau einmal auftritt. Damit können wir z.B. eine Permutation in der Form

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

angeben. Steht diese für die Permutation f und für g die Permutation

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$$

so ist die Verknüpfung $g \circ f$ durch

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

gegeben, während $f \circ g$ durch

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

geben ist. Daran sieht man daß die Gruppe der Permutationen nicht kommutativ ist.

Wieviele Elemente hat die Permutationsgruppe? Nun ja, wir können in die zweite Reihe eine beliebige Anordnung der n Zahlen schreiben. An die erste Stelle können wir eine beliebige der n Zahlen aufschreiben, dies gibt n Möglichkeiten. Für die zweite Stelle haben wir dann noch $(n-1)$-Möglichkeiten, dies ergibt zusammen schon $n(n-1)$ Möglichkeiten. Führen wir das fort, so ergeben sich $n(n-1)(n-2)\cdots 1$ Möglichkeiten. Also gilt

Satz 2.1.5
Die Gruppe der Permutationen der Zahlen $1, \ldots, n$ hat $n!$ Elemente. Wir bezeichnen diese Gruppe mit S_n.

Eine alternative Schreibweise für Permutationen ist manchmal einfacher handhabbar. Wir schreiben eine Zeile und beginnen mit der 1. Dann schreiben wir $f(1)$, dann $f(f(1))$ usw. Schließt sich die Permutation, bevor alle Elemente aufgeschrieben sind, so machen wir eine Klammer herum und fahren fort, indem wir mit der ersten noch nicht aufgeführten Zahl weiter machen. Wir nennen dies die *Zyklenschreibweise* der Permutation.

Die obigen Beispiele aus S_3 nehmen dann die Form an

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1,2)(3)$$

$$g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1,2,3),$$

$$g \circ f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1,3)(2)$$

und

$$f \circ g \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (1)(2,3).$$

Für die Gruppe S_3 schreiben wir alle Permutationen in beiden Schreibweisen auf:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = (1)(2)(3)$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1,2)(3)$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1,3)(2)$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (1)(2,3)$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1,2,3)$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1,3,2)$$

Aufgabe 2.1.6
Man schreibe die Permutation

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 7 & 3 & 1 & 6 & 5 & 4 \end{pmatrix}$$

in der Zyklenschreibweise.

Ein weiteres wichtiges Beispiel für Gruppen sind die Bewegungsgruppen regelmäßiger geometrischer Figuren.

Beispiel 2.1.7
Wir beginnen mit einem einfachen Beispiel: gegeben sei ein gleichseitiges Dreieck D als Teilmenge des $\mathbb{R}^2$. Eine affine lineare Abbildung

$$L : \mathbb{R}^2 \to R^2 : X \mapsto Ax + b,$$

wobei A eine orthogonale Matrix und $b \in \mathbb{R}^2$ ein Vektor ist, heißt Bewegung *auf $\mathbb{R}^2$. Ist L eine Bewegung, so daß $LD = D$ ist,so heißt L eine Bewegung des Dreiecks D. Die Menge der Bewegungen einer geometrischen Figur F wird als* Symmetriegruppe *von F bezeichnet. Für das gleichseitige Dreieck hat die Symmetriegruppe 6 Elemente, wir beobachten, daß die Anzahl der Elemente mit der der Gruppe S_3 übereinstimmt, hat dies eine Bedeutung?*

Beispiel 2.1.8
Nun kommt ein Beispiel, das etwas komplizierter ist. Wir betrachten das Tetraeder im $\mathbb{R}^3$ und wieder die Menge der Bewegungen. Wir kommen auf 12 Elemente. Wir sehen in diesem Beispiel, daß es Elemente gibt, die bei wiederholter Anwendung das neutrale Elemente ergibt.

Schreibweise: Gruppen können multiplikativ oder additiv geschrieben werden. Dies ist reine Konvention ohne inhaltliche Bedeutung. Wir stellen gegenüber:

Bedeutung	$(G, +)$	$(G, \cdot)$
Neutrales Element	0	1
Inverses Element	$-g$	g^{-1}
Summe	$g_1 + g_2$	$g_1 g_2$
Vielfache	ng	g^n

Wir werden uns im Allgemeinen an die multiplikative Schreibweise halten. Nur bei speziellen Gruppen, in denen traditionell additive Schreibweise üblich ist, z.B. $\mathbb{Z}$, werden wir dies auch so schreiben.

Definition 2.1.9
Sei G eine Gruppe in multiplikativer Schreibweise, $g \in G$. Gibt es ein Element $n \in \mathbb{N}$ mit $g^n = 1$, so hat das Element g endliche Ordnung, *das kleinste $n \in \mathbb{N}$ mit dieser Eigenschaft heißt* Ordnung *von g.*

Beispiel 2.1.10
Spiegelungen haben Ordnung zwei, die Drehungen des gleichseitigen Dreiecks Ordnung 3, die Permutation $(134)(2)$ hat Ordnung 3.

Aufgabe 2.1.11
Man bestimme die Ordnungen alle Elemente der Bewegungsgruppe eines Tetraeders. Wie sieht das bei den anderen regelmäßigen Körpern im $\mathbb{R}^3$ aus?

Zu jeder algebraischen Struktur, wie z.B. einem Vektorraum oder einer Gruppe, betrachtet man die Abbildungen, die diese Struktur erhalten. Diese Sichtweise der Mathematik ist überaus erfolgreich, das starre Festhalten versperrt aber manchmal den Blick auf die eigentlichen Inhalte.

Bemerkung 2.1.12
Deshalb vielleicht nochmals ein Blick zurück. Wir haben Gruppen definiert, Beispiele für Gruppen gesehen und die Beschäftigung mit Gruppen durch das Streben Gleichungen lösen zu wollen motiviert. Jedoch haben Gruppen wesentlich mehr Anwendungsbereiche. Wir wollen hier nur einige nennen:

1. Beschreibung von Symmetrien: Anwendungen: reguläre Körper, Platonische Körper, Beschreibung von Symmetrien von Kristallen, Schneeflocken usw.

2. Beschreibung der Symmetrien von Mustern: Alhambra (Kunst), Strömungszustände von Flüssigkeiten z.B. im Taylor- und Bénardproblem (Strömungsmechanik).

3. Untersuchung von Beulzuständen mechanischer Strukturen (Kugeln unter gleichmäßigen äußeren Druck).

4. Quantenmechanik: Beschreibung der Zustände, Transformation.

5. Physik und Mechanik: geometrische Randbedingungen (Rollen von Scheiben usw.).
6. Physik: Transformationsgruppen, Eichinvarianz, Galileiinvarianz, Lorenztransformation.
7. Eisenbahnverkehr: Musterbildung auf der Schiene, Polygonisierung des Rades.
8. Geophysik: Erdmagnetismus.
9. Biologie: Musterbildung bei Tieren.
10. Biologie/Physik/Chemie: Spiralwellen und deren Dynamik.
11. Biologie: Gangarten von n-Füßlern, speziell für $n = 2, 4, 6$.

Definition 2.1.13
Es seien G_1, G_2 zwei Gruppen. Eine Abbildung von $h : G_1 \to G_2$ heißt Homomorphismus, *wenn folgende Bedingungen erfüllt sind:*

Hom 1 $h(xy) = h(x)h(y)$;

Hom 2 $h(x^{-1}) = (h(x))^{-1}$.

Definition 2.1.14
Es seien G_1 und G_2 zwei Gruppen, $h : G_1 \to G_2$ ein Homomorphismus. Die Menge

$$H = \left\{ x \in G_1 \;\middle|\; h(x) = 1 \right\}$$

wird als Kern *des Homomorphismus bezeichnet.*

Dafür hat man die folgenden elementaren Eigenschaften.

Satz 2.1.15
Sind G_1 und G_2 zwei Gruppen und ist $h : G_1 \to G_2$ ein Homomorphismus, so ist der Kern von h eine Untergruppe von G_1. Speziell ist $1 \in H$. h ist genau dann injektiv, wenn $H = \{1\}$ ist. Ist h bijektiv, so existiert eine Umkehrabbildung $h^{-1} : G_2 \to G_1$, welche ebenfalls ein Gruppenhomomorphismus ist.

Beweis. Sind $x, y \in H$, so ist

$$h(xy^{-1}) = h(x)h(y^{-1}) = 1 \cdot (h(y))^{-1} = 1.$$

Ist $H \neq \{1\}$, so ist h offenkundig nicht injektiv, also impliziert injektiv, $H = \{1\}$. Andererseits folgt aus $H = \{1\}$ und $h(x) = h(y)$, daß $h(x)(h(y))^{-1} = 1$ und

$$1 = h(x)(h(y))^{-1} = h(xy^{-1}).$$

Also ist $xy^{-1} = 1$ und daher $x = y$.

Wir müssen noch beweisen, daß h^{-1} ein Gruppenhomomorphismus ist. Seien also $w, z \in G_2$. Dann existieren x, y mit $h(x) = w, h(y) = z$ und

$$h(xy^{-1}) = h(x)h(y)^{-1},$$

also ist

$$h^{-1}(h(xy^{-1})) = h^{-1}(h(x)h(y)^{-1})$$

oder

$$xy^{-1} = h^{-1}(wz^{-1})$$

oder

$$h^{-1}(w)(h^{-1}(z))^{-1} = h^{-1}(wz^{-1}).$$

Dies war zu beweisen. □

Definition 2.1.16
Ein bijektiver Homomorphismus wird als Isomorphismus *bezeichnet. Gibt es einen Isomorphismus zwischen zwei Gruppen G_1 und G_2 so nennt man die Gruppen G_1 und G_2* isomorph.

Aufgabe 2.1.17
Man zeige, die Bewegungsgruppe $\mathbb{D}_3$ eines gleichseitigen Dreiecks und die Permutationsgruppe S_3 sind isomorph.

Abstrakte Gruppentheorie betrachtet isomorphe Gruppen als im wesentlichen gleich. Ziel ist es, Gruppen „bis auf Isomorphie“ zu charakterisieren. Dieses Ziel ernsthaft zu verfolgen sprengt den Rahmen dieser Vorlesung. Daher wollen wir nur einige einfache Bemerkungen in diese Richtung machen.

Definition 2.1.18
Eine Teilmenge $H \subset G$ heißt Untergruppe *der Gruppe G, wenn H bezüglich der Verknüpfung in G eine Gruppe ist.*

Definition 2.1.19
(a) Eine Teilmenge A erzeugt *die Untergruppe H, wenn jedes Element in H als Produkt von Elementen aus A oder deren Inversen geschrieben werden kann.*
(b) Eine Gruppe heißt zyklisch, *wenn es ein Element $a \in G$ gibt, so daß $A = \{a\}$ die Gruppe G erzeugt.*

Beispiel 2.1.20

1. Die Gruppe der Drehungen R_3 eines gleichseitigen Dreiecks ist eine Untergruppe der Bewegungsgruppe eines Dreiecks. Sie ist zyklisch.

2. Die Gruppe $\mathbb{Z}$ ist zyklisch. Jedes Element ist Vielfaches (das vielfache ist ja die Potenz in additiver Schreibweise) der $1 \in \mathbb{Z}$ oder der -1.

3. Jede Gruppe der Form $\mathbb{Z}/q\mathbb{Z}$ ist zyklisch. Das Element $[1]_q$ erzeugt die Gruppe.

4. Ist p eine Primzahl, so ist $\mathbb{Z}/p\mathbb{Z} \setminus \{[0]_p\}$ eine (multiplikative) Gruppe (folgt aus unseren früheren Überlegungen). Diese Gruppe ist zyklisch (dies werden wir noch sehen).

Aufgabe 2.1.21
Zu $p \in \mathbb{Z}$, p prim, finde man ein $1 < q < p$, so daß $[q]_p$ die Gruppe $\mathbb{Z}/p\mathbb{Z} \setminus \{[0]_p\}$ erzeugt.

Definition 2.1.22
Ist G eine endliche Gruppe, so bezeichnen die Anzahl ihrer Elemente als Ordnung *und schreiben dafür $|G|$. Entsprechende Schreibweise wenden wir auch auf Untergruppen an.*

Definition 2.1.23
Es sei G eine Gruppe, $H \subset G$ eine Untergruppe. Für $g \in G$ betrachten wir nun die Menge $gH = \left\{gh \,\middle|\, h \in H\right\}$. Für $g \in G$ gH heißt Linksnebenklasse *von H. Entsprechend definieren wir Rechtsnebenklassen als Mengen der Form $Hg = \left\{hg \,\middle|\, h \in H\right\}$.*

Satz 2.1.24
Ist H eine Untergruppe der Gruppe G und sind $g_1, g_2 \in G$, so ist entweder

$$g_1H = g_2H$$

oder

$$g_1H \cap g_2H = \emptyset.$$

Entsprechendes gilt für Rechtsnebenklassen.

Beweis. Wir zeigen, aus $g_1H \cap g_2H \neq \emptyset$ folgt

$$g_1H = g_2H.$$

Angenommen $g_1H \cap g_2H \neq \emptyset$. Das heißt

$$g_1h_1 = g_2h_2 \text{ für gewisse } h_1, h_2 \in H.$$

Dann ist $h_2 = g_2^{-1}g_1h_1$. Ist nun $g_2h \in g_2H$, dann ist

$$\begin{aligned} g_2h &= g_2h_2h_2^{-1}h = g_2g_2^{-1}g_1h_1(g_2^{-1}g_1h_1)^{-1}h \\ &= g_1h_1(g_2^{-1}g_1h_1)^{-1}h. \end{aligned}$$

Da $h_1(g_2^{-1}g_1h_1)^{-1}h \in H$ liegt, ist auch $g_2h \in g_1H$ und damit ist $g_2H \subset g_1H$. Durch Vertauschen von g_1, g_2 im vorigen Argument erhält man $g_1H \subset g_2H$ und die beiden Mengen sind gleich. □

Wir fassen zusammen:

Satz 2.1.25
Die Menge der Linksnebenklassen bildet eine disjunkte Zerlegung in Teilmengen (Nebenklassen).

Beweis. Folgt sofort aus dem zuvor Gesagtem. □

Bemerkung 2.1.26
Ist H endlich, so haben je zwei Linksnebenklassen die gleiche endliche Anzahl von Elementen, nämlich $|H|$. Ist H nicht endlich, sind je zwei Linksnebenklassen bijektiv aufeinander abbildbar (*gleichmächtig*).

Diese Konstruktion liefert sofort:

Satz 2.1.27
Ist G eine endliche Gruppe und H eine Untergruppe, so ist die Anzahl der Elemente $|H|$ in H ein Teiler von $|G|$.

Beweis. Jede Nebenklasse von H hat $|H|$ Elemente, also ist

$$|G| = q|H|,$$

wobei q die Anzahl der Nebenklassen ist. □

Satz 2.1.28
Hat eine Gruppe Primzahlordnung, so ist sie zyklisch.

Beweis. Sei $g \in G, g \neq 1$ und H die von $A = \{g\}$ erzeugte Untergruppe. Dann ist $1 < |H|$ ein Teiler der Primzahl $|G|$, also $|G| = |H|$. □

Definition 2.1.29
Ist jede Rechtsnebenklasse von H auch eine Linksnebenklasse, so nennt man H einen Normalteiler. *Wir definieren dann folgende Rechenregeln für die Nebenklassen*

$$(g_1H)(g_2H) = g_1g_2H.$$

Die Menge der Nebenklassen bezeichnen wir mit G/H.

Satz 2.1.30
Ist H ein Normalteiler von G, so wird G/H mit der angegebenen Verknüpfung zur Gruppe.

Wir erinnern uns an die Rechenregeln für $[x]_p + [y]_p$!

Beweis. Der erste Schritt ist zu zeigen, daß die Verknüpfung *wohldefiniert* ist. Dies bedeutet, daß das Ergebnis von $(g_1H)(g_2H)$ nicht von der speziellen Wahl von g_1, g_2 abhängt. Sind also d_1 und d_2 in der jeweils gleichen Nebenklasse wie g_1 bzw. g_2, so ist

$$g_1g_2H = d_1d_2H.$$

Warum? g_1 ist in der gleichen Nebenklasse genau dann, wenn es ein h_1 gibt, mit $d_1 = g_1h_1$ und entsprechend auch für $d_2 = g_2h_2$. dann ist

$$d_1d_2H = g_1h_1g_2h_2H = g_1h_1g_2H = g_1g_2\tilde{h}H = g_1g_2H,$$

da H ein Normalteiler und damit Linksnebenklassen auch Rechtsnebenklassen sind. Alle Eigenschaften einer Gruppe für G/H folgen unmittelbar aus den Gruppeneigenschaften für G. □

Satz 2.1.31
Eine Untergruppe H ist genau dann ein Normalteiler, wenn für jedes $g \in G$ und jedes $h \in H$ gilt

$$ghg^{-1} \in H.$$

Beweis. Zu $h \in H$ existiert ein $h_1 \in H$ mit $gh = h_1 g$. Dann ist $ghg^{-1} = h_1 \in H$.

Umgekehrt ist $ghg^{-1} \in H$, so folgt $gh \in Hg$ und $gH \subset Hg$. Entsprechend zeigt man $Hg \subset gH$ und $gH = Hg$. □

Satz 2.1.32
Sind G, H Gruppen und ist

$$f : G \to H$$

ein Gruppenhomomorphismus, so ist $\ker f$ *ein Normalteiler von G.*

Beweis. Sei $H = \ker f$ und $g \in G$. Dann ist

$$f(ghg^{-1}) = f(g)f(h)f(g)^{-1} = f(g)fg)^{-1} = 1.$$

Dies beweist die Behauptung. □

Wir kommen nochmals auf die Permutationen der Menge $\{1, \ldots, n\}$ zurück. Jeder Permutation f können wir eine $n \times n$-Matrix $A = (a_{ij})$ zuordnen durch

$$a_{ij} = 1 \text{ dann und nur dann wenn } f(i) = j \text{ ist,}$$

ansonsten setzen $a_{ij} = 0$. Eine solche Matrix hat in jeder Spalte und in jeder Zeile genau eine 1, sonst sind alle $a_{ij} = 0$.

Definition 2.1.33
Eine Matrix mit genau einer 1 *in jeder Zeile und Spalte und sonst nur Nullen wird als* Permutationsmatrix *bezeichnet.*

Aufgabe 2.1.34
Die Menge der $n \times n$-Permutationsmatrizen bildet eine Gruppe.

Aufgabe 2.1.35
Die Zuordnung, die eine Permutation f auf die entsprechende Matrix M_f abbildet ist ein Gruppenhomomorphismus $T : S_n \to \mathbb{P}(n)$, wobei $\mathbb{P}(n)$ für die Menge der Permutationsmatrizen steht. Ist T ein Isomorphismus? Man beweise die entsprechenden Aussagen (sofern sie korrekt sind, ansonsten gebe man ein Gegenbeispiel!)

Aufgabe 2.1.36
Man schreibe die Permutationsmatrizen für alle Permutationen in S_3.

Aufgabe 2.1.37
Untergruppen zyklischer Gruppen sind zyklisch.

Aufgabe 2.1.38
Wieviele Gruppen (bis auf Isomorphie) gibt es für

$$|G| = 1, 2, 3, 4, 5, 6?$$

2.2 Ringe

Wir wollen uns nur kurz mit dieser wichtigen algebraischen Struktur beschäftigen. Ringe haben zwei Verknüpfungen, meistens als $+, \cdot$ geschrieben. Bezüglich der ersten bilden sie eine Gruppe und die zweite wird mit der ersten durch Distributivgesetze verbunden. Formal schreiben wir

Definition 2.2.1
Eine Menge R mit zwei Verknüpfungen $+, \cdot$, also formal ein Tripel $(R, +, \cdot)$, ist ein Ring*, wenn es bezüglich der ersten Verknüpfung eine abelsche Gruppe ist, die zweite Verknüpfung genügt dem Assoziativgesetz und ist mit der ersten durch*

Dis 1 $x \cdot (y + z) = x \cdot y + x \cdot z$

Dis 2 $(y + z) \cdot x = y \cdot z + z \cdot x$

verbunden. Die erste Verknüpfung nennen wir Addition, die zweite Multiplikation. Das neutrale Element in $(R, +)$ wird mit 0 bezeichnet. Gibt es bezüglich der zweiten Verknüpfung ein neutrales Element, so nennen wir dieses 1. Ist die Multiplikation kommutativ, so bezeichnen wir den Ring als kommutativ.

Beispiel 2.2.2

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ *sind Ringe.*

2. *Ist R ein Ring, so ist die Menge aller formalen Ausdrücke der Form*

$$P(X) = \sum_{n=0}^{\infty} a_n X^n$$

mit $a_i \in R$ und nur endlich vielen $a_i \neq 0$ ein Ring. Die Addition zweier Elemente $P_1(X) = \sum_{i=1}^{\infty} a_i^{(1)} X^i$, $P_2(X) = \sum_{i=1}^{\infty} a_i^{(2)} X^i$ ist definiert durch

$$P_1(X) + P_2(X) = \sum_{i=1}^{\infty} (a_i^{(1)} + a_i^{(2)}) X^i$$

und die Multiplikation durch

$$P_1(X) \cdot P_2(X) = \sum_{k=1}^{\infty} \left(\sum_{\nu=1}^{k} a_\nu^{(1)} a_{k-\nu}^{(2)} \right) X^k.$$

Ein solcher Ring wird als Polynomring *bezeichnet, man schreibt dafür $R[X]$. Spezielle Ringe erhält man aus den vorherigen durch diese Konstruktion: $\mathbb{Z}[X]$, $\mathbb{Q}[X]$, $\mathbb{R}[X]$, $\mathbb{C}[X]$.*

3. *$\mathbb{Z}/q\mathbb{Z}$ ist ein Ring.*

4. *$R = \mathbb{Z} + i\mathbb{Z} = \left\{ x + iy \;\middle|\; x, y \in \mathbb{Z} \right\}$ ist der Ring der Gaußschen Zahlen*

5. *Die Menge der $n \times n$-Matrizen bildet einen Ring. Dieser Ring ist nicht kommutativ.*

6. *Die Quaternionen bilden einen Ring.*

Aufgabe 2.2.3
Man beweise die oben gemachte Aussage, daß für einen Ring R die Menge der Polynome $R[X]$ einen Ring bildet. Man begründe jeden Schritt sorgfältig.

Satz 2.2.4
In einem Ring R gelten für $a, b \in R$ die folgenden Regeln:

1. *$a \cdot 0 = 0 \cdot a = 0$;*

2. *$a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$;*

3. *$(-a) \cdot (-b) = ab$;*

4. *$(-1) \cdot a = -a$.*

Beweis. Es gilt

$$a \cdot 0 + a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 = a \cdot 0 + 0$$

und daher $a \cdot 0 = 0$.

Für die zweite Aussage betrachten wir

$$a \cdot b + a \cdot (-b) = a \cdot (b + (-b)) = a \cdot 0 = 0$$

nach (1). Also ist $a \cdot (-b) = -(ab)$. Entsprechend beweist man die andere Aussage.

Die dritte Aussage folgt (fast) direkt aus der zweiten Aussage. Wie?

Aus der zweiten Aussage folgt

$$(-1) \cdot a = -(1 \cdot a) = -a,$$

da $1 \cdot a = a$. □

Bemerkung 2.2.5
Man beachte, daß nicht (notwendig) alle vertrauten Regeln gelten:

1. $(a - b)(a + b) = a^2 - b^2$ *ist eine dieser Regeln.*

2. $ab = 0$ *impliziert* $a = 0$ *oder* $b = 0$.

Ist $ab = 0$, $a \neq 0$, $b \neq 0$ so nennt man a, b *Nullteiler*

Aufgabe 2.2.6
Zu beiden Regeln suche man jeweils einen Ring und zwei Elemente, so daß die entsprechende Aussage nicht gilt.

Definition 2.2.7
Eine Teilmenge eines Ringes, die bezüglich der beiden Verknüpfungen selbst wieder ein Ring ist, wird als Unterring *bezeichnet.*

In einem Ring haben nicht alle Elemente $a \neq 0$ ein multiplikatives Inverses. (Beispiel: $5 \in \mathbb{Z}$). Daher betrachtet man die Teilmenge all der Elemente mit multiplikativem Inversen.

Definition 2.2.8
$R^* = \left\{ a \in R \;\middle|\; a \text{ hat multiplikatives Inverses} \right\}$.

Satz 2.2.9
R^* ist bezüglich $\cdot$ eine Gruppe.

Beweis. Folgt sofort aus $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$. □

Definition 2.2.10
Eine Teilmenge I eines Ringes R heißt Ideal, *wenn sie bezüglich der Addition eine Untergruppe ist, und bezüglich der Multiplikation gilt*

$$a \in I, r \in R \text{ impliziert } r \cdot a, a \cdot r \in I.$$

Ideale spielen eine wichtige Rolle, dies vor allem wegen des folgenden Satzes, der die wichtigsten Eigenschaften der den Ringen zugeordneten Abbildungen sammelt. Zunächst jedoch die wichtigsten Begriffe.

Definition 2.2.11

1. *Es seien R_1, R_2 zwei Ringe und $f : R_1 \to R_2$ eine Abbildung. Diese Abbildung heißt* Ringhomomorphismus, *falls es ein Homomorphismus der zugrundeliegenden additiven Gruppen ist und $f(r_1 \cdot r_2) = f(r_1) \cdot f(r_2)$.*

Definition 2.2.12
Ist $f : R_1 \to R_2$ ein Ringhomomorphismus, so ist

$$\ker f = \left\{ a \in R_1 \;\middle|\; f(a) = 0 \right\}.$$

Lemma 2.2.13
Ist $f : R_1 \to R_2$ ein Ringhomomorphismus, so ist $\ker f$ *ein Ideal in R_1.*

Beweis. Sind $r_1, r_2 \in \ker f$, so ist (beachte f ist auch ein Gruppenhomomorphismus) $r_1 + r_2 \in \ker f$.

Daher müssen wir nur zeigen, daß mit $i \in \ker f$ und $r \in R$ auch $r \cdot i \in \ker f$. Es gilt $f(r \cdot i) = f(r) \cdot f(i) = f(r) \cdot 0 = 0$. □

Die Ideale übernehmen die Rolle der normalen Untergruppen aus der Gruppentheorie.

Beispiel 2.2.14
Die Menge

$$2\mathbb{Z} = \left\{ 2z \;\middle|\; z \in \mathbb{Z} \right\}$$

ist ein Ring, ein Unterring von $\mathbb{Z}$ und ein Ideal im Ring $\mathbb{Z}$. Entsprechend den Nebenklassen bilden wir nun den Quotienten $\mathbb{Z}/2\mathbb{Z}$ und dies bildet einen Ring, denn wir definieren (wie schon vor längerem beobachtet) $[1]_2 \cdot [1]_2 = [1]_2$ und entsprechend die anderen Produkte.

Eine Verallgemeinerung dieser Konstruktion liefert die Quotientenbildung R/I, wobei R ein Ring und I ein Ideal ist. Da R bezüglich der Addition eine abelsche Gruppe ist, ist I als Untergruppe normal und rein gruppentheoretisch der Quotient R/I erklärt.

Satz 2.2.15
Auf R/I ist die Multiplikation wohldefiniert.

Beweis. Zu zeigen ist also, ist $r_1 - r_2 \in I$, $t_1 - t_2 \in I$, dann ist

$$r_1 t_1 - r_2 t_2 \in I.$$

Es gilt

$$r_1 t_1 - r_2 t_2 = r_1 t_1 - r_1 t_2 + r_1 t_2 - r_2 t_2 = r_1(t_1 - t_2) + (r_1 - r_2) t_2 \in I,$$

denn beide Summanden sind in I. Also ist die Nebenklasse des Produktes je zweier Elemente aus zwei gegebenen Nebenklassen gleich und damit können wir die Produktbildung auf Nebenklassen übertragen. □

Zwei wichtige Klassen von Idealen spielen eine entscheidende Rolle.

Definition 2.2.16

1. *Ein* Primideal, *ist ein Ideal I mit $a \cdot b \in I$, impliziert $a \in I$ oder $b \in I$.*

2. *Ein* maximales Ideal *I ist eine Teilmenge eines Ringes, die erstens ein Ideal ist und für die gilt, ist $I \subset J$, $I \neq J$ und J ein Ideal, so ist $J = R$.*

Satz 2.2.17
Beliebige Durchschnitte von Idealen sind Ideale.

Beweis. Folgt sofort aus der Definition. □

Beispiel 2.2.18

1. *Ist $p \in \mathbb{Z}$ eine Primzahl, so ist $p\mathbb{Z}$ ein Primideal und ein maximales Ideal.*

2. *Wir ordnen einem Polynom $P \in \mathbb{R}[X]$ die Abbildung*

$$\mathbb{R} \to \mathbb{R} : x \mapsto P(x)$$

zu. Ist $Z \subset \mathbb{R}$ eine endliche Teilmenge, so ist

$$I = \left\{ P \in \mathbb{R}[X] \;\middle|\; P(x) = 0 \text{ für alle } x \in Z \right\}$$

ein Ideal in $\mathbb{R}[X]$. Weshalb? Ist $P_1, P_2 \in I$, so verschwindet auch $P_1(x)+ P_2(x)$ auf der Menge Z und mit $P(x) = 0$ für alle $x \in Z$ ist auch

$$Q(x)P(x) = 0 \text{ für alle } x \in Z$$

und $Q \in \mathbb{R}[X]$. Also ist I ein Ideal. I ist prim, falls Z nur aus einem Punkt besteht. Denn ein Produkt zweier Funktionen ist in einem Punkt Null genau dann, wenn eine der beiden Funktion dort verschwindet.

3. *Jedem Polynom kann man das kleinste Ideal zuordnen, das dieses Polynom enthält.*

2.3 Polynome

In diesem Abschnitt wollen wir die Betrachtung von Polynomen noch etwas vertiefen.

Definition 2.3.1
Es sei R ein Ring, z.B. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ oder $\mathbb{C}$, und $P \in R[X]$ ein Polynom,

$$P(X) = \sum_{n\in\mathbb{N}} a_n X^N,$$

wobei nur endlich viele $a_i \neq 0$ sind. Der Grad von P ist das maximale n mit $a_n \neq 0$. Wir schreiben dafür $\mathrm{grad}(P)$. Das Nullpolynom hat Grad -1.

Lemma 2.3.2
Sind P, Q Polynome, so ist

$$\mathrm{grad}(P+Q) \leq \max\left(\mathrm{grad}(P), \mathrm{grad}(Q)\right)$$

$$\mathrm{grad}(P \cdot Q) = \mathrm{grad}(P) + \mathrm{grad}(Q).$$

Beweis. Klar! □

Definition 2.3.3
Ein Polynom $Q \in R[X]$ ist Vielfaches *von P, falls es ein Polynom $T \in R[X]$ gibt, mit $P \cdot T = Q$. Das Polynom P ist dann ein* Teiler *von Q.*

Lemma 2.3.4
Sind P, Q Polynome, mit $\mathrm{grad}(P) \geq \mathrm{grad}(Q) > 0$, so gibt es Polynome S, R mit $\mathrm{grad}(R) < \mathrm{grad}(Q)$ und

$$P = SQ + R.$$

Beweis. Ist $\mathrm{grad}\, P \geq \mathrm{grad}\, Q$, so gibt es eine Zahl $a \in R$ mit

$$\mathrm{grad}(P - aX^{\mathrm{grad}\, P - \mathrm{grad}\, Q} Q) < \mathrm{grad}(P).$$

Wiederholtes Anwenden dieser Formel liefert den Beweis. □

Damit kann man den euklidischen Algorithmus für Polynomringe definieren und den größten gemeinsamen Teiler zweier Polynome definieren und algorithmisch berechnen.

Definition 2.3.5
Ein gemeinsamer Teiler S der Polynome P, Q heißt größter gemeinsamer Teiler *von P, Q falls S unter allen gemeinsamen Teilern maximalen Grad hat.*

Der Euklidische Algorithmus angewandt auf Polynome liefert einen größten gemeinsamen Teiler (der natürlich nicht eindeutig bestimmt ist).

Definition 2.3.6
Ist $f \in R[X]$, so heißt $x \in R$ eine Nullstelle *von f, falls $f(x) = 0$ ist.*

Satz 2.3.7
x ist genau dann eine Nullstelle, wenn $(X - x)$ ein Teiler von f ist.

Beweis. Ist $(X - x)$ ein Teiler, so hat f die Gestalt $f(X) = (X - x)g(X)$. Offenkundig ist dies für $X = x$ Null.

Für die Rückrichtung betrachten wir

$$f(X) = S(x)(X - x) + R(X)$$

und $\mathrm{grad}(R) < 1$. Also ist R konstant. Da $f(x) = 0$ und $S(X)(X - x)$ bei $X = x$ verschwindet, ist $R = 0$. □

Definition 2.3.8
Ein Polynom P vom Grad mindestens 1 ist irreduzibel, *wenn es keine Teiler S hat mit $1 \leq \mathrm{grad}(S) < \mathrm{grad}(P)$.*

Beispiel 2.3.9
1. *Lineare Polynome sind irreduzibel.*

2. *In $\mathbb{Q}[X]$ ist $P(X) = X^2 + 1$ irreduzibel, jeder nichttriviale Teiler wäre linear und daher eine Nullstelle. Für $x \in \mathbb{Q}$ ist aber $P(x) > 1$.*

3. *In $R = \mathbb{Z}/2\mathbb{Z}[x]$ ist $P(X) = X^4 + X + 1$ irreduzibel. Da $P(0) = P(1) = 1$, gibt es keine Nullstelle und also keine linearen Teiler. Eine Faktorisierung der Form $P(X) = (X^2 + aX + b)(X^2 + cX + d)$, $a, b, c, d \in \mathbb{Z}/2\mathbb{Z}$ führt auf*

   $$X^4 + X + 1 = X^2 + (a + c)X^3 + (b + d + ac)X^2 + (ad + bc)X + bd.$$

   Dann ist $b = d = 1$ und $a = c$. Mit $0 = b + d + ac = ac$ ist $a = 0$ oder $b = 0$ und dies ist ein Widerspruch zu $ad + bc = 1$.

Wie im ersten Kapitel erhalten wir folgende Aussage.

Lemma 2.3.10
Zwei Polynome $P, Q \in R[X]$ sind genau dann relativ prim, wenn es Polynome S, T gibt mit

$$PS + QT = 1.$$

Beweis. Jeder gemeinsame Teiler teilt 1 und ist damit konstant.

Die Gegenrichtung wird wie bei relativ primen Zahlen durch den Euklidischen Algorithmus bewiesen. □

Satz 2.3.11
Sind $P, Q, T \in R[X]$ und P, Q relativ prim, so folgt aus $P|QT$, daß $P|T$.

Beweis. Nach der vorherigen Beobachtung gilt es gibt Polynome U, V mit

$$UP + VQ = 1,$$

also $UPT + VQT = T$. Nun teilt P das Produkt UPT und ebenso VQT (nach Voraussetzung), also auch die rechte Seite, nämlich T. □

Satz 2.3.12
Jedes Polynom kann als Produkt irreduzibler Polynome geschrieben werden. Diese Zerlegung ist eindeutig bis auf die Reihenfolge und Multiplikation mit Konstanten, d.h. ist $P \in R[X]$, so ist

$$P = Q_1 \cdot Q_2 \cdot \ldots \cdot Q_n$$

mit irreduziblen Faktoren $Q_k \in R[X]$. Gibt es eine zweite solche Darstellung

$$P = R_1 \cdot R_2 \cdot \ldots \cdot R_m,$$

so ist $m = n$ und zu jedem Q_k existiert ein R_l und eine Konstante $q_k \in R$ mit $Q_k = q_k R_l$.

Beweis. Wir zeigen zunächst die Darstellbarkeit, danach die Eindeutigkeit. Wir zeigen dies per Induktion. Lineare Polynome sind irreduzibel, dies ist der Anfang unserer Induktion. Angenommen, es sei gezeigt, daß jedes Polynom vom Grad höchstens n als Produkt irreduzibler Polynome geschrieben werden kann. Sei f vom Grad $n+1$. Ist f irreduzibel, so ist nichts zu zeigen, im anderen Fall ist f Produkt zweier Polynome vom Grad mindestens 1, sagen wir $f = gh$. Dann ist $1 \leq \mathrm{grad}(g) < \mathrm{grad}(f)$ und $1 \leq \mathrm{grad}(h) < \mathrm{grad}(f)$ und damit sind diese in der behaupteten Form darstellbar. Das überträgt sich auf das Produkt. Ein ganz ähnliches Induktionsargument zeigt die Eindeutigkeit. □

2.4 Eine Anwendung: Verschieberegister

Eine der wichtigen Probleme der Softwareindustrie ist die Erzeugung einer Folge von Zufallszahlen. Eine Methode beruht auf sogenannten Verschieberegistern, die wir jetzt vorstellen wollen. Was ist ein Verschieberegister. Dazu sind eine Reihe von Registern nebeneinander angeordnet, etwa wie es das folgende Schema zeigt, jedes Register enthält eine Zahl.

$$\boxed{g_{k-1}} \quad \boxed{g_{k-2}} \quad \boxed{g_{k-3}} \quad \cdots \quad \boxed{g_{k-n}}$$

Nach einem Zeitschritt werden alle Registerinhalte nach rechts verschoben, das rechteste wird ausgegeben und links wird ein neues Element erzeugt. Wir erhalten die folgende Erweiterung des Schemas

$$\boxed{\text{Input}} \to \boxed{g_{k-1}} \to \boxed{g_{k-2}} \to \boxed{g_{k-3}} \to \cdots \to \boxed{g_{k-n}} \to \boxed{\text{Output}}$$

Der Input links wird aus den gegenwärtigen Registerinhalten erzeugt, indem man für jedes Register einen Koeffizienten (von links gezählt $s_{n-1}, s_{n-2}, \ldots, s_0$) vorab ausgewählt hat, und nun bildet

$$g_k = s_{n-1}g_{k-1} + s_{n-2}g_{k-2} + \cdots + s_0 g_{k-n}.$$

Hat man am Anfang eine Belegung der Register festgelegt und die Koeffizienten ein für alle Mal bestimmt, erzeugt diese Maschine eine Folge von Zahlen. Wir schreiben für das sogenannte *Shiftpolynom*

$$S(X) = \sum_{k=0}^{n-1} s_k X^k.$$

Definition 2.4.1
Sei $S \in R[X]$ ein Polynom vom Grad $n-1$ über dem Ring R. Das Shiftregister *über R mit Shiftpolynom S ist die Abbildung, die einer Anfangsbelegung*

$g_0, g_1, \ldots, g_{n-1}$ mit n Elementen in R eine Folge g_i von Elementen in R zuordnet durch die Vorschrift

$$g_k = s_{n-1}g_{k-1} + s_{n-2}g_{k-2} + \ldots + s_0 g_{n-k} \ (n \leq k).$$

Beispiel 2.4.2
Sei $R = \mathbb{Z}/2\mathbb{Z}$ und $S(X) = 1+X+X^3$. Starten wir mit der Anfangsbelegung $g_0 = 1, g_1 = 0, g_2 = g_3 = 0$, so erhalten wir die Folge

$$1, 0, 0, 0, 1, 1, 0, 1, 1, \ldots.$$

Wir wollen nun den Output nach $k > n$ Verschiebungen untersuchen. Dazu brauchen wir die Polynome

$$f = \sum_{j=0}^{n-1} \left(g_j - \sum_{i=1}^{j} s_{n-i} g_{j-i} \right) X^j$$

und

$$T = s_{n-1}X + s_{n-2}X^2 + \cdots s_0 X^n.$$

Man beachte den Unterschied zwischen S, T.

Satz 2.4.3
In einem Verschieberegister wird der $k+1$-te Output durch den Koeffizienten von X^k im Polynom

$$(1 + T + T^2 + \cdots + T^k)f$$

gegeben.

Beweis. Wir wollen den Beweis nur andeuten.

Wir betrachten die formale Reihe

$$\sum_{i=0}^{\infty} g_i X^i,$$

die natürlich kein Polynom ist, deren Koeffizient bei X^k aber gerade der gewünschte Output ist. Da wir uns im Moment für den $k+1$-ten Output g_k interessieren und da dieser ja schon durch den Anteil $G = \sum_{i=1}^{k} g_i X^i$ beschrieben wird, liegt es nahe, dieses Polynom zu betrachten. Die Behauptung des Satzes ist gezeigt, wenn wir die Gleichheit

$$G = (1 + T + T^2 + \cdots + T^k)f \text{ bis auf Vielfache von } X^{k+1}$$

beweisen.

Bis auf Vielfache von X^{k+1} ist

$$(1-T)G = f.$$

Dann ist aber

$$(1+T+\cdots+T^k)(1-T)G = (1+T+\cdots+T^k)f$$

bis auf Vielfache von X^{k+1}. Da $[(1+T+\cdots+T^k)(1-T) = 1-T^{k+1} = 1$ bis auf Vielfache von X^{k+1} folgt die behauptete Gleichheit. $\square$

Bei der Erzeugung von Zufallszahlen ist es ein Ziel, daß die Folge entweder keine Periode oder aber eine möglichst große Periode hat.

Um die Periode der von einem Verschieberegister erzeugten Folge berechnen zu können, wollen wir noch ein wenig Lineare Algebra investieren und mit einem speziellen Ring $R = \mathbb{R}$ arbeiten. Wir betrachten das Shiftpolynom S und ordnen ihm eine Matrix zu, nämlich

$$A = \begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & s_0 \\ 1 & 0 & 0 & \ldots & 0 & s_1 \\ 0 & 1 & 0 & \ldots & 0 & s_2 \\ & & & \ldots & & \\ 0 & 0 & 0 & \ldots & 1 & s_{n-1} \end{pmatrix}.$$

Beim Übergang vom k-ten Zustand zum $(k+1)$-sten Zustand wird der Inhalt der Register

$$(g_{k-n}, \ldots, g_{k-1}) \mapsto (g_{k-n+1}, \ldots, g_k) = (g_{k-n}, \ldots, g_{k-1})A$$

abgebildet.

Satz 2.4.4
Das Minimalpolynom von A ist $X^n - S$.

Beweis. Lineare Algebra. $\square$

Satz 2.4.5
Die Periode d des Verschieberegisters ist ein Teiler von d, falls das Minimalpolynom ein Teiler von $X^d - 1$ ist.

2.5 Restklassenringe

Ist P ein Polynom I das zugehörige Ideal, dann ist $R[X]/I$ der Restklassenring modulo P, wir schreiben auch $R[X]/(P)$.

Es gelten alle Rechenregeln, die wir am Anfang der Vorlesung angegeben haben.

Invertierbare Elemente

Satz 2.5.1
Ist P irreduzibel, so sind alle Elemente invertierbar.

2.6 Körper

Definition 2.6.1
Ein Ring K, in dem jedes von Null verschiedene Element invertierbar ist, heißt Körper.

In einem Körper bildet die Menge der von Null verschiedenen Elemente eine multiplikative Gruppe.

Beispiel 2.6.2
Beispiele für Körper sind $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ (nicht endlich), $K = Z/pZ$, wobei p eine Primzahl ist. Ist p prim und P irreduzibel, so ist

$$Z/pZ(P).$$

ein Körper.

Satz 2.6.3
Ist K ein Körper mit p Elementen und ist $P \in K[X]$ irreduzibel mit $\operatorname{grad}(P) = n$, so hat $K[X]/(P)$ p^n Elemente.

Schließlich notieren wir noch den Satz

Satz 2.6.4
Jeder endliche Körper hat für ein $n \in \mathbb{N}$ und eine Primzahl p p^n Elemente. Ein solcher Körper ist isomorph zu $K[X]/(P)$, wobei $K = \mathbb{Z}/p\mathbb{Z}$ und $P \in K[X]$ ein irreduzibles Polynom ist.

Betrachtet man ein irreduzibles Polynom zweiten Grades über $\mathbb{Z}/2\mathbb{Z}$ so erhält man den Körper mit 4 Elementen. Damit kann man die vollständige Verknüpfungstafel für diesen Körper aufschreiben.

Aufgabe 2.6.5
In einem Körper K *betrachten wir die Summe*

$$\underbrace{1+1+\cdots+1}_{n-mal} = n\cdot 1.$$

Das kleinste n*, so daß* $n\cdot 1 = 0$ *ist nennen wir die Charakteristik von* K*. Existiert kein solches* $n \in \mathbb{N}$*, so sagen wir die Charakteristik ist unendlich. Man zeige, die Charakteristik eines Körpers ist entweder unendlich oder eine Primzahl.*