Inhaltsverzeichnis

Kapitel 2

Gruppen, Ringe, Körper

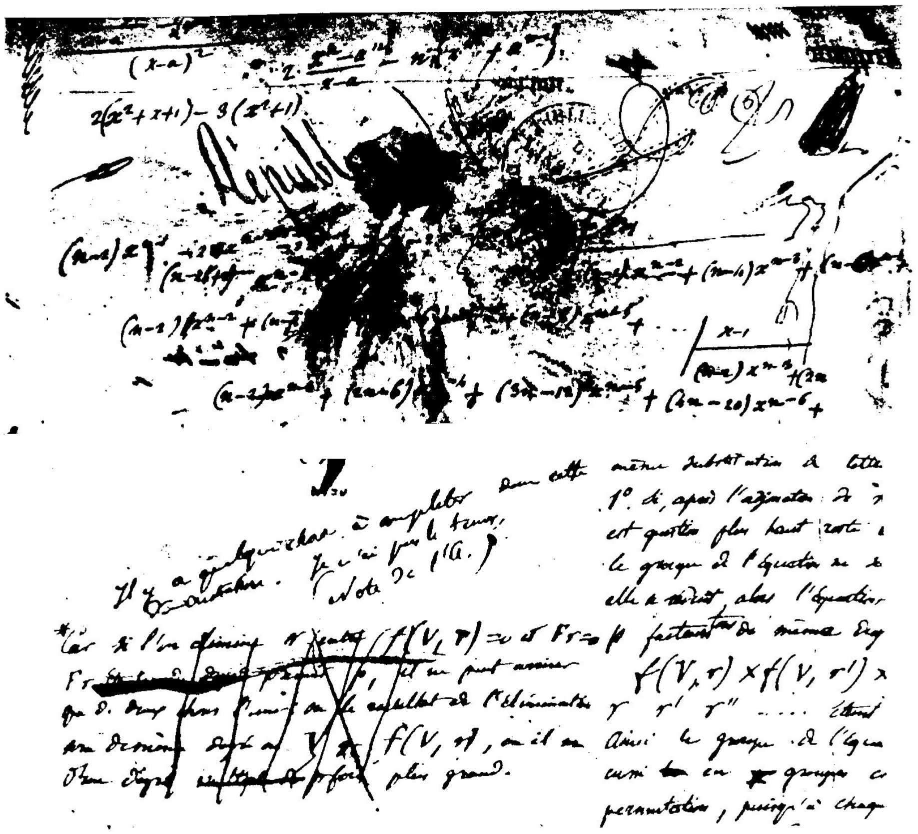
Wir haben mit den Bijektionen einer Menge M mathematische Objekte kennengelernt, die sich mittels Komposition „$\circ$“ so verknüpfen lassen, dass das Resultat wieder eine Bijektion ist. Ferner genügt diese Verknüpfung dem Assoziativgesetz, es existieren eine neutrale Abbildung id sowie zu jeder Bijektion f eine Umkehrabbildung (Inverse) f^{-1}. Die gleichen Eigenschaften weist auch die Multiplikation der rationalen, von Null verschiedenen Zahlen auf, und es lassen sich viele weitere Beispiele finden (siehe später in diesem Kapitel).

Daher ist es ökonomisch, solchermaßen gleichgeartete Beispiele unter einem neuen Begriff mittels Abstrahierung zu erfassen, hier dem Begriff der Gruppe. Die Bezeichnung Gruppe (franz. groupe) stammt von [1] dem genialen Evariste Galois (1811–1832), der mit seiner Lösung des Problems, notwendige und hinreichende Bedingungen für die Auflösung algebraischer Gleichungen durch Radikale anzugeben,

E. Galois

[1]Galois' Lösung war so revolutionär, dass sie von den zeitgenössischen Mathematikern nicht verstanden wurde. Galois hatte 1829 ein Manuskript mit der Darstellung seiner Methode bei der Akademie eingereicht. Obwohl der für die Prüfung zuständige A. Cauchy sich selbst mit Permutationen beschäftigt hatte, hat er die Galoissche Arbeit nicht verstanden. Denn aus einem in den Archiven der Akademie befindlichen Brief geht hervor, dass Cauchy am 18.01.1830 in der Akademie über Galois' Arbeit vortragen wollte. Er entschuldigte sich jedoch wegen Krankheit, kündigte dabei den Vortrag für die folgende Woche an, sprach dort jedoch über eigene Arbeiten und erwähnte Galois niemals (?) wieder. Cauchy hatte sich wohl überhoben. Galois reichte seine Arbeit im Februar 1830 erneut bei der Akademie ein. Diesmal ging sie jedoch wundersamerweise unter der Federführung von J. Fourier verloren. Am weitesten kam noch das dritte 1831 bei der Akademie eingereichte Papier:

bahnbrechend für die Auffassung von Mathematik als einer Theorie der Strukturen wurde.[2]



Je n'ai pas le temps

Letzteres wurde auf Empfehlung von Poisson zurückgewiesen. An eine kritische Randbemerkung schrieb Galois (wahrscheinlich in der Nacht vor dem Duell) die legendären Worte „On jugera“ (Die Nachwelt wird darüber richten), an eine andere Stelle „Je n'ai pas le temps“ (Ich habe nicht die Zeit ...). Die mathematische Fachwelt brauchte fast 40 Jahre, ehe die Galoissche Theorie verstanden wurde. Das widerlegt auch die bisweilen leichtfertig geäußerte These, dass gute Mathematik eo ipso gute Didaktik bedeute.

[2]„Seit Beginn des (19.) Jahrhunderts hat der Kalkül einen solchen Grad an Kompliziertheit erreicht, dass jeder Fortschritt durch dieses Mittel unmöglich geworden ist ... In dieser Abhandlung werden die weitestgehenden der bisher verwendeten kalkulatorischen Methoden als Spezialfälle (einer allgemeineren Betrachtungsweise) aufgefasst ... “ E. Galois, manuscripts, ed. J. Tannery, Paris 1918, p. 25, 26.

Es werden also, sobald man genügend verschiedene Beispiele dafür hat, neue, abstrakte Strukturen axiomatisch durch Angabe ihrer Eigenschaften definiert. Objektorientierten Programmierern ist Ähnliches von dem Entwurf von Klassen, Templates usw. her bekannt.

2.1 Definitionen : (**Binäre**) **Verknüpfung** $\circ$ auf einer Menge M wird eine Abbildung $M \times M \to M$ mit $(a, b) \mapsto a \circ b$ für alle a, $b \in M$ genannt.

(i) Wenn stets $a \circ b = b \circ a$ ist, so heißt die Verknüpfung **kommutativ**.

(ii) Eine Menge A mit einer bzw. mehreren Verknüpfungen heißt eine **algebraische Struktur**.

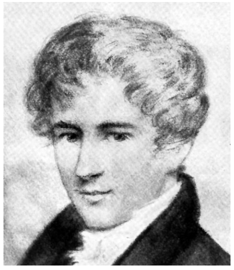
(iii) Eine Menge H mit einer assoziativen (siehe 1.12(ii)) Verknüpfung $\circ$ heißt eine **Halbgruppe**.

(iv) Ein Element $e \in H$ heißt **neutrales Element** oder **Einselement**, wenn $e \circ x = x \circ e = x$ für alle $x \in H$ gilt.

(v) Eine Halbgruppe mit neutralem Element wird ein **Monoid** genannt.

(vi) Ein Element b eines Monoids M heißt ein **Inverses** von $a \in M$, wenn $b \circ a = a \circ b = e$ gilt. Das Inverse b wird dann mit a^{-1} bezeichnet.

(vii) Ein Monoid G heißt eine **Gruppe**, wenn jedes Element von G ein Inverses besitzt. $\circ$ wird dann die **Gruppenmultiplikation** genannt und von nun an auch so geschrieben, also „ab“ statt „$a \circ b$“.



N. H. Abel (1802-1829)

(viii) Wenn die Gruppenmultiplikation kommutativ ist, so heißt G **kommutative** oder **abelsche Gruppe**.

(ix) Die Kardinalzahl $|G|$ von G – d.i. im endlichen Fall die Anzahl der Elemente von G – heißt die **Ordnung** von G.

(x) G heißt **endliche Gruppe**, wenn $|G| < \infty$ ist.

2.2 Bemerkungen :

(i) In einem Monoid ist das neutrale Element eindeutig bestimmt, eine Halbgruppe kann also höchstens ein neutrales Element enthalten.
Denn: Wenn e, e' neutrale Elemente sind, so gilt $e \circ e' = e'$, aber auch $= e$. Mithin ist $e = e'$.

(ii) Zu jedem Gruppenelement ist das Inverse eindeutig bestimmt.
Denn: Wenn a^{-1}, α^{-1} Inverse zu a sind, so gilt $a^{-1} = a^{-1}e = a^{-1}a\alpha^{-1}$ $= e\alpha^{-1} = \alpha^{-1}$.

(iii) Sei G eine Gruppe. Dann gilt

$$\forall (a,b) \in G \times G \;\; \exists_1 (x,y) \in G \times G : xa = b \wedge ay = b \quad .$$

Denn: $x := ba^{-1}$ löst $xa = b$, und $x_1 a = x_2 a$ impliziert $x_1 = x_2$. Analog für y.

(iv) Es seien G Gruppe und $a, a_1, a_2, \ldots, a_n \in G$. Dann gilt $(a^{-1})^{-1} = a$ und $(a_1 a_2 \ldots a_n)^{-1} = a_n^{-1} \ldots a_2^{-1} a_1^{-1}$.

(v) In der Gruppe G vermitteln die Abbildungen $x \mapsto xa$, $x \mapsto ax$ und $x \mapsto x^{-1}$ Bijektionen von G auf sich.
Denn: $x \mapsto xa$ ist surjektiv wegen der Existenz der Lösung von $xa = b$ und injektiv wegen der Eindeutigkeit der Lösung. Schließe analog für $x \mapsto ax$. Schließlich ist $x \mapsto x^{-1}$ eine Abbildung α mit $\alpha \circ \alpha = \mathrm{id}_G$, also ist α nach 1.13 bijektiv.

2.3 Beispiele :

(i) $\mathbb{N}$ ist bezüglich der Multiplikation ein kommutatives Monoid (1 ist das neutrale Element).

(ii) $2\mathbb{N} := \{2, 4, 6, \ldots\}$ ist bezüglich der Multiplikation eine Halbgruppe, aber kein Monoid. Informatiker betrachten bisweilen Halbgruppen, z.B. stetige Matrixhalbgruppen mit stetiger Zeit bei Markoffprozessen.[3]

[3] Siehe G. Pflug: Stochastische Modelle in der Informatik, p. 29ff.

(iii) $\mathbb{Z}$ ist bezüglich der Addition eine abelsche Gruppe.

(iv) $\mathbb{Q}^* := \mathbb{Q} \setminus \{0\}$ ist eine (abelsche) Gruppe bezüglich der Multiplikation.

Nebenstehend Abels Denkmal in Oslo. Der Genius tritt die Ignoranten in den Staub

(v) Die Menge aller Bijektionen von M, sogenannter **Permutationen** oder auch **Transformationen** der Menge M, ist eine i.a. nichtabelsche Gruppe bezüglich der Komposition, oft als S_M bezeichnet. Wenn $|M|$ endlich ist, etwa $= n$, nimmt man als Bezeichnung für die n Elemente von M gern $1, 2, \ldots, n$, spricht von ihnen als den **Ziffern** der Permutationsgruppe und nennt letztere die **symmetrische Gruppe** S_n vom **Grad** n. Nach 1.21 hat die Gruppe die Ordnung $n!$.

(vi) Rechnen wir doch einmal in der symmetrischen Gruppe S_3: Eine Schreibweise für Permutationen besteht im Untereinandersetzen von Urbild und Bild: $g_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $g_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $g_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, $g_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $g_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, $g_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ sind also die Elemente von S_3. g_1 ist das neutrale Element, g_4 ist das Inverse von g_5. $g_2 g_3 \neq g_3 g_2$ zeigt, daß S_3 nicht abelsch ist. Wir lesen das Produkt von Permutationen von links nach rechts!

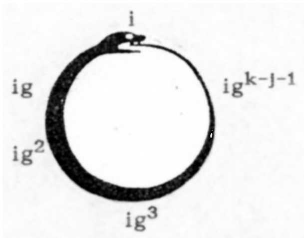
(vii) Die Menge T aller Drehungen, die ein reguläres Tetraeder mit sich zur Deckung bringen, ist bzgl. der Komposition eine Gruppe der Ordnung 12, die sog. **Tetraedergruppe**. (Sie tritt z.B. als Drehgruppe des Methan-Moleküls auf). In den Anwendungen (z.B. Kristallographie) treten oft auch die **Oktaedergruppe** O mit $|O| = 24$ und die **Ikosaedergruppe** I mit $|I| = 60$ auf.

Für den Umgang mit Permutationen ist oft die sogenannte **Zyklenschreibweise** zweckmäßig: Es seien G eine Permutationsgruppe, $g \in G$ und i eine der Ziffern. Statt $gg \cdots g$ (n Faktoren) schreiben wir g^n. Die Ziffern $i, ig, ig^2, \ldots$ bilden die sogenannte **Bahn** oder das **Orbit** von i unter g. Bei endlich vielen Ziffern ist notwendig $ig^k = ig^j$ für gewisse $k, j \in \mathbb{N}$. Sei etwa $k \geq j$ und es sei die erste Situation beim Durchlaufen der Ziffern von j nach k, wo eine solche Gleichheit auftritt. Dann ist $ig^{k-j} = i$, und

$i, ig, ig^2, \ldots, ig^{k-j-1}$ sind paarweise verschieden. Wir schreiben für den Teil der Permutation, der diese Ziffern betrifft:

$$\begin{pmatrix} i & ig & ig^2 & \ldots & ig^{k-j-1} \\ ig & ig^2 & ig^3 & \ldots & i \end{pmatrix} := \begin{pmatrix} i & ig & ig^2 & \ldots & ig^{k-j-1} \end{pmatrix} \quad .$$

Letzteres Gebilde heißt ein **Zyklus**, da das Orbit zyklisch durchlaufen wird. Wie eine Schlange, die sich in den Schwanz beißt!



Die Ziffernmenge eines Zyklus von g ist also die Bahn einer Ziffer. Zur gleichen Bahn unter g zu gehören definiert eine Äquivalenzrelation auf der Menge der Ziffern. Daher gilt:

2.4 Satz : Jede Permutation von endlich vielen Ziffern lässt sich bis auf Reihenfolge eindeutig als Produkt elementfremder Zyklen schreiben.

2.5 Gruppentafeln :

Eine **m × n-Matrix** (g_{ij}) meint ein Rechteckschema: $\begin{bmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ g_{m1} & g_{m2} & \cdots & g_{mn} \end{bmatrix}$

Wenn $|G| = n$ ist, so lässt sich die Gruppe G durch eine $n \times n$-Matrix (g_{ij}) folgendermaßen beschreiben: Wir rändern die Matrix mit einer oberen Zeile $g_1, g_2, \ldots, g_n$ sowie einer entsprechenden ersten Spalte und verabreden $g_{ij} := g_i g_j \in G$. Die geränderte Matrix heißt dann die **Gruppentafel** von G.
Zum Beispiel für $n = 2$: Sei etwa g_1 das neutrale Element. Dann ist notwendig $g_{21} = g_2$ und somit $g_{22} = g_1$ (wegen der Bijektivität von $x \mapsto x g_2$). Die Bijektivität der Abbildungen $x \mapsto g_i x$ und $x \mapsto x g_j$ (2.2 (v)) begründet den

Slogan: In jeder Zeile (bzw. Spalte) der Gruppentafel tritt jedes Gruppenelement genau einmal auf.

Für $n = 3$ hat die Gruppentafel folgendes Aussehen:

*	g_1	g_2	g_3
g_1	g_1	g_2	g_3
g_2	g_2	g_3	g_1
g_3	g_3	g_1	g_2

Überlege, dass sich für $n = 4$ kombinatorisch zwei essentiell verschiedene Möglichkeiten ergeben!

Um zu zeigen, dass die konstruierten Tafeln auch Gruppen darstellen, müssen wir jeweils nur noch das Assoziativgesetz nachweisen. Denn es gilt:

2.6 Satz : Sei G eine Menge mit einer Verknüpfung $*$ so, dass

(i) das Assoziativgesetz gilt und

(ii) zu jedem $a, b \in G \quad x, y \in G$ existieren mit $a * x = b$ und $y * a = b$.

Dann ist G eine Gruppe.

Beweis: Wegen (ii) existiert zu jedem $a \in G$ eine „individuelle Linkseins" $e_1(a)$, d.h. $e_1(a) * a = a$. Dann ist $e_1(a)$ aber sogar „universelle Linkseins", d.h. es gilt $e_1(a) * g = g$ für alle $g \in G$; denn wegen der Lösbarkeit von $a * x = g$ gilt: $e_1(a) * g = e_1(a) * a * x = a * x = g$. Ebenso existiert eine universelle Rechtseins e_2. Linkseins ist gleich Rechtseins, denn es gilt $e_1 = e_1 * e_2 = e_2$. Also existiert eindeutig (2.2 (i)) das neutrale Element e. Die Voraussetzung (ii) impliziert ebenso die Existenz des Inversen: Denn zu a existiert ein Linksinverses $l(a)$ und ein Rechtsinverses $r(a)$: $l(a) * a = e = a * r(a)$. Nun ist aber $l(a) = l(a) * e = l(a) * a * r(a) = e * r(a) = r(a)$, also existiert das Inverse zu a. $\square$

2.7 Definition : Es seien G eine Gruppe und U eine Teilmenge von G. U heißt **Untergruppe** von G, geschrieben $U < G$, wenn U bezüglich der in G erklärten Gruppenmultiplikation wieder eine Gruppe ist.

2.8 Bemerkungen :

(i) Wenn U eine nichtleere, bezüglich der Multiplikation abgeschlossene Teilmenge einer Gruppe G ist, für die mit jedem $u \in U$ auch $u^{-1} \in U$ gilt, so ist $U < G$.
Denn: Die Assoziativität ist für U erfüllt, da die Assoziativität in G gilt. Inverse existieren nach Voraussetzung. Es ist aber auch $e = uu^{-1} \in U$.

(ii) Wenn U eine endliche nichtleere, bezüglich der Multiplikation abgeschlossene Teilmenge einer Gruppe G ist, so ist $U < G$.
Denn: Für $a \in U$ ist $x \mapsto xa$ nach 2.2 (v) eine Injektion $U \to U$, wegen der Endlichkeit von U sogar eine Bijektion. Also ist $xa = a$ in U lösbar und somit $e \in U$. Aber auch $xa = e$ ist in U lösbar und somit $a^{-1} \in U$.

(iii) Jede Gruppe besitzt zwei triviale Untergruppen , nämlich $\{e\}$ und G.

2.9 Definitionen : Sei G eine Gruppe und seien $A, B \subset G$.
$AB := \{ab : a \in A \wedge b \in B\}$ heißt das **Komplexprodukt** von A und B. Ist speziell $A = \{a\}$, so schreiben wir aB statt $\{a\}B$ (analog Ab). Wir verwenden auch die Bezeichnung $A^{-1} := \{a^{-1} : a \in A\}$. Wenn $U < G$ und $g \in G$ ist, so heißt Ug eine **Rechtsnebenklasse** von U in G.

2.10 Beispiel : Sei $G = (\mathbb{Z}, +)$ die additive Gruppe von $\mathbb{Z}$, und sei $U := 5\mathbb{Z} := \{0, \pm 5, \pm 10, \dots\}$. Die Rechtsnebenklassen von U in G sind die Kongruenzklassen mod 5: $U = U + 0$, $U + 1 = \{\dots, -9, -4, 1, 6, 11, \dots\}$, $U + 2$, $U + 3$, $U + 4$.

2.11 Bemerkungen : Sei G eine Gruppe. Dann gilt:

(i) $U < G \leftrightarrow UU = U \ \wedge \ U = U^{-1}$

(ii) Wenn $U < G$ und $g, h \in G$ sind, so gilt: $h \in Ug \leftrightarrow Ug = Uh$.
Denn: Wenn $h \in Ug$, etwa $h = ug$, ist, so gilt $Uh = Uug = Ug$. Wenn $Ug = Uh$ ist, so ist $h = eh \in Uh = Ug$.

(iii) Für $U < G$ und alle $g \in G$ gilt $|Ug| = |U| = |gU|$.

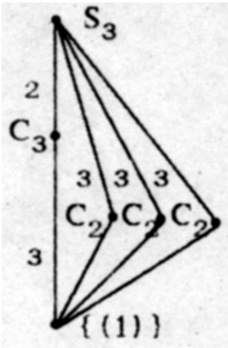
(iv) Sei $U < G$. Wir definieren eine Relation ρ auf G: Es gelte $a\rho b$, wenn a und b in derselben Rechtsnebenklasse von U sind. ρ ist eine Äquivalenzrelation. Wir erhalten also eine Partition von G in Rechtsnebenklassen: $G = \dot{\bigcup\limits_{g \in \mathcal{S}}} Ug$, wobei $\mathcal{S}$ ein sogenannter **Schnitt** oder ein **Rechts-Repräsentantensystem** ist, nämlich eine Menge, die aus jeder Äquivalenzklasse genau ein Element enthält.
Es gilt auch $G = \dot{\bigcup\limits_{g \in \mathcal{S}}} g^{-1}U$. Also: Die Kardinalität der Menge der Rechtsnebenklassen ist gleich der Kardinalität der Menge der Linksnebenklassen, der sogenannte **Index** von U in G, geschrieben $|G : U|$.
Denn: $Ug = Uh \leftrightarrow h \in Ug \leftrightarrow h = ug$ für ein $u \in U \leftrightarrow h^{-1} = g^{-1}u$ für ein $u \in U \leftrightarrow h^{-1}U = g^{-1}U$.

Damit ist der folgende Satz bewiesen:
2.12 Satz von Lagrange : Sei G eine Gruppe mit $U < G$.

Dann ist $|G| = |U| \cdot |G : U|$.

Slogan: Die Ordnung der Untergruppe ist ein Teiler der Gruppenordnung.

Übung (zu 2.9 bis 2.11): Nachfolgend sind alle nichttrivialen Untergruppen von S_3 aufgeführt:
$C_3 = \{(\ 1\ \ 2\ \ 3\ ), (\ 1\ )\}$,
$C_2^{(1)} = \{(\ 1\ \ 2\ ), (\ 1\ )\}$,
$C_2^{(2)} = \{(\ 2\ \ 3\ ), (\ 1\ )\}$,
$C_2^{(3)} = \{(\ 1\ \ 3\ ), (\ 1\ )\}$.



Schreibe für jede der vier nichttrivialen Untergruppen die Partition von S_3 in Linksnebenklassen bzw. in Rechtsnebenklassen auf. Nebenstehend der Graph des Untergruppenverbandes von S_3. ($|_B^A n$ bedeutet $B < A$ mit Index $|A : B| = n$).

2.13 Definitionen : G_1, G_2 seien Gruppen.

(i) Eine Abbildung $\varphi : G_1 \to G_2$ heißt ein **Gruppenmorphismus** (früher auch: **Gruppenhomomorphismus**) , wenn für φ die sogenannte **Relationstreue** gilt, d.h. wenn $\varphi(gh) = \varphi(g)\varphi(h)$ für alle $g, h \in G$ gilt.

Die Bedingung der Relationstreue kann auch geometrisch durch die sog. **Kommutativität** des nebenstehenden Diagramms dargestellt werden.

$$\begin{tikzcd} G_1 \times G_1 \arrow[r, "\circ"'] \arrow[d, "\varphi"'] \arrow[dr, phantom, "\circlearrowright"] & G_1 \arrow[d, "\varphi"] \\ G_2 \times G_2 \arrow[r, "\circ"'] & G_2 \end{tikzcd}$$

(ii) Ist $G_1 = G_2$, so heißt der Morphismus auch **Endomorphismus**.

(iii) Ein injektiver Morphismus heißt **Monomorphismus**.

(iv) Ein surjektiver Morphismus heißt **Epimorphismus**.

(v) Ein bijektiver Morphismus heißt **Isomorphismus** , geschrieben $G_1 \simeq G_2$. Wir sagen auch: es besteht **Isomorphie** zwischen G_1 und G_2. Oder: G_1 ist **isomorph** zu G_2.

(vi) Wenn $G_1 = G_2$ ist, so heißt ein Isomorphismus auch **Automorphismus**.

(vii) Wir definieren schließlich noch: **Kern** $\varphi := \{x : x \in G_1 \wedge \varphi(x) = e_{G_2}\}$.

> **Slogan** (für Relationstreue): Das Bild des Produktes ist gleich dem Produkt der Bilder.

Morphismen sind die an die algebraische Struktur des Urbildes angepaßten Abbildungen (Denke an die Relationstreue!). Sie „vergröbern“ u.U. die algebraische Struktur, ohne sie jedoch „in ihrem Wesen“ zu zerstören. Ein Maß für die „Vergröberung“ ist die Größe des Kerns. Bei einem Homomorphismus φ werden jeweils genau die Elemente einer Nebenklasse des Kerns auf dasselbe Bildelement abgebildet:

2.14 Bemerkungen : Sei $\varphi : G \to H$ ein Gruppenmorphismus. Dann gelten:

(i) $\varphi(e_G) = e_H$ (denn $e_G x = x$ impliziert $\varphi(e_G)\varphi(x) = \varphi(x)$),

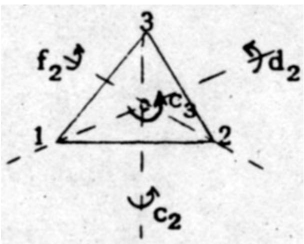
(ii) $\varphi(x^{-1}) = \varphi(x)^{-1}$ (Wende φ auf $xx^{-1} = e$ an),

(iii) wenn $U < G$, so ist $\varphi(U) < \varphi(G)$ (wegen (i), (ii). Die Abgeschlossenheit bzgl. der Multiplikation ist klar),

(iv) wenn $U' < H$, so ist $\varphi^{-1}(U') < G$,

(v) Kern $\varphi < G$.

2.15 Beispiele :



Die Gruppe D_3 der Drehungen eines gleichseitigen Dreiecks (im 3-dimensionalen Raum) heißt **Diedergruppe** (der Ordnung 6). Die Gruppe S_3 aller Permutationen von 3 Ziffern heißt **symmetrische Gruppe** vom Grad 3. Es besteht eine Isomorphie $S_3 \simeq D_3$: $e \leftrightarrow (1)(2)(3)$, $c_2 \leftrightarrow (1\ 2)$, $d_2 \leftrightarrow (2\ 3)$, $f_2 \leftrightarrow (1\ 3)$, $c_3 \leftrightarrow (1\ 2\ 3)$, $c_3^2 \leftrightarrow (1\ 3\ 2)$.

Die Abbildung, die e, c_3, c_3^2 auf (1) und c_2, d_2, f_2 auf $(1\ 2)$ abbildet, ist ein Morphismus $D_3 \to S_2$, der kein Isomorphismus ist.

Wir gehen jetzt zu algebraischen Strukturen mit zwei Verknüpfungen über. Als Modell haben wir zunächst den Bereich $\mathbb{Z}$ der ganzrationalen Zahlen vor Augen mit seinen beiden Verknüpfungen Addition und Multiplikation.

2.16 Definitionen : Eine algebraische Struktur R mit $R \neq \emptyset$ und den beiden Verknüpfungen $+$ und $\cdot$, genannt Addition und Multiplikation, heißt ein **Ring**, wenn folgende Eigenschaften gelten:

(i) $(R, +)$ ist eine abelsche Gruppe ,

(ii) die Multiplikation ist assoziativ ,

(iii) $\forall a,b,c \in R : a(b+c) = ab + ac \ \wedge \ (a+b)c = ac + bc$.

Wenn $1 \in R$ existiert mit $1x = x1 = x$ für alle $x \in R$, so heißt R ein **Ring mit Eins**.

Ein Element u eines Ringes mit Eins heißt eine **Einheit**, wenn u sowohl ein multiplikatives Rechtsinverses wie auch ein multiplikatives Linksinverses besitzt, d.h. es existieren $a, b \in R$ mit $au = 1$ und $ub = 1$.

Wenn die Multiplikation im Ring R kommutativ ist, so heißt R **kommutativer Ring**. Eine bezüglich beider Verknüpfungen relationstreue Abbildung von Ringen heißt ein **Ringhomomorphismus** oder **-morphismus** . Analog werden **Ringisomorphismus**, **-epimorphismus** , ... definiert.

2.17 Beispiele :

(i) $(\mathbb{Z}, +, \cdot)$ und $(\mathbb{Q}, +, \cdot)$ sind kommutative Ringe mit 1. $\{+1, -1\}$ und $\mathbb{Q} \setminus \{0\} =: \mathbb{Q}^*$ sind die Einheitenmengen von $\mathbb{Z}$ bzw. $\mathbb{Q}$.

(ii) $n\mathbb{Z} := \{nz : n \in \mathbb{N} \wedge z \in \mathbb{Z}\}$ ist für $n \in \mathbb{N} \setminus \{1\}$ ein kommutativer Ring ohne 1.

(iii) $\mathbb{Z}_n := \{\widehat{0}, \widehat{1}, \ldots, \widehat{n-1}\}$ ist ein kommutativer Ring mit 1, wobei $\widehat{i}$ die Kongruenzklasse $n\mathbb{Z} + i$ modulo n ist, der sog. **Restklassenring** modulo n. Dabei wird mit den Restklassen $\widehat{i}$ so gerechnet wie mit den kleinsten positiven Resten $i \mod n$. Also z.B. in $\mathbb{Z}_6$: $4 \cdot 3 = 12 \equiv 0 \mod 6$, daher ist $\widehat{4} \cdot \widehat{3} = \widehat{0}$. Die Einheitenmenge von $\mathbb{Z}_6$ ist $\{\widehat{1}, \widehat{5}\}$.

(iv) Sei R ein kommutativer Ring mit Eins (letztere als 1 geschrieben). Wir definieren: $R[x] := \{(a_0, a_1, a_2, \ldots) : a_i \in R, i \in \mathbb{N} \cup \{0\}$, nur endlich viele $a_i \neq 0\}$, $(a_0, a_1, \ldots) = (b_0, b_1, \ldots) :\leftrightarrow a_i = b_i$ für alle $i \in \mathbb{N} \cup \{0\}$, $(a_0, a_1, \ldots) + (b_0, b_1, \ldots) :\leftrightarrow (a_0 + b_0, a_1 + b_1, \ldots)$, $(a_0, a_1, \ldots) \cdot (b_0, b_1, \ldots) :\leftrightarrow (a_0 b_0, a_0 b_1 + a_1 b_0, \ldots, a_0 b_k + a_1 b_{k-1} + \ldots + a_k b_0, \ldots)$ (an der k-ten Stelle, kurz $\sum\limits_{m+n=k} a_m b_n$).

Es ist leicht nachzuprüfen, dass $R[x]$ mit den solchermaßen definierten Verknüpfungen ein kommutativer Ring mit Eins ist. Zum Beispiel rechnen wir ein Distributivgesetz nach:

$$\begin{aligned}
&(\dots, a_i, \dots)[(\dots, b_i, \dots) + (\dots, c_i, \dots)] \\
&= (\dots, a_i, \dots)(\dots, b_i + c_i, \dots) \\
&= (\dots, \sum_{m+n=i} a_m(b_n + c_n), \dots) \\
&= (\dots, \sum_{m+n=i} a_m b_n + \sum_{m+n=i} a_m c_n, \dots) \\
&= (\dots, \sum_{m+n=i} a_m b_n, \dots) + (\dots, \sum_{m+n=i} a_m c_n, \dots) \\
&= (\dots, a_i, \dots)(\dots, b_i, \dots) + (\dots, a_i, \dots)(\dots, c_i, \dots) \quad .
\end{aligned}$$

Wir betrachten eine Abbildung α, die durch $\alpha((a_0, a_1, a_2, \dots)) := a_0 + a_1 x + a_2 x^2 + \dots$ definiert sei. $R[x]$ wird wegen der Abbildung α der **Polynomring** über R in der **Unbestimmten** x genannt. Wenn wir nämlich im Bildbereich von α rechnen, wie wir das Rechnen mit Polynomen auf der Schule gelernt haben, so ist α ein Ringisomorphismus. x erfüllt keine algebraische Gleichung $\sum_{j=0}^{n} a_i x^i = 0$, heißt auch **nichtalgebraisch** oder **transzendent** über R. So ist z.B. π transzendent über $\mathbb{Q}$. Aber $\sqrt{2}$ ist algebraisch über $\mathbb{Q}$, da es Lösung der algebraischen Gleichung $x^2 - 2 = 0$ ist. Die Einheiten von $R[x]$ sind genau die Einheiten von R.

(v) Eine **n × n-Matrix** ist ein Gebilde der Gestalt $\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$, kurz (a_{ij}) geschrieben. Die a_{ij} heißen **Einträge** oder **Koeffizienten** der Matrix.

Sei $M_{n,n}(R)$ die Menge aller $n \times n$-Matrizen mit Koeffizienten aus dem Ring R. $M_{n,n}(R)$ wird ein Ring, wenn Addition und Multiplikation folgendermaßen definiert werden: $(a_{ij}) + (b_{ij}) := (a_{ij} + b_{ij})$, $(a_{ij})(b_{ij}) := (\sum_{\nu=1}^{n} a_{i\nu} b_{\nu j})$.

Slogan: Die Matrizenaddition erfolgt komponentenweise. Die Matrizenmultiplikation erfolgt nach dem Motto „Zeile mal Spalte“.

2.18 Bemerkungen : Sei R ein Ring. Dann gelten:

(i) $0r = r0 = 0$ für alle $r \in R$. **Denn:** $0r = (0+0)r = 0r + 0r$, also $0r = 0$ wegen der Eindeutigkeit des neutralen Elements der additiven Gruppe.

(ii) $(-a)b = a(-b) = -ab$ für alle $a, b \in R$. **Denn:** wegen $0 = 0b = (a + (-a))b = ab + (-a)b$ ist $(-a)b = -ab$.

(iii) $(-a)(-b) = ab$ für alle $a, b \in R$. **Denn:** Es ist $(-a)(-b) = -(a(-b)) = -(-ab)$, also $= ab$ (2.2 (vi)).

(iv) Wenn $\varphi : R \to R'$ ein Ringhomomorphismus ist, so ist $\varphi(R)$ ein Ring.

(v) Wenn $\varphi : R \to R'$ ein Ringhomomorphismus und R ein Ring mit Eins ist, so ist $\varphi(1)y = y\varphi(1) = y$ für alle $y \in \varphi(R)$.

Achtung: $\varphi(1)$ ist damit noch nicht notwendig Eins in R'! Betrachte zum Beispiel die **natürliche Injektion** $\varphi(a) := (a, 0)$ von $\mathbb{Z}$ in $\mathbb{Z} \times \mathbb{Z}$, wobei letztere Menge vermöge komponentenweise definierter Addition und Multiplikation ein Ring ist (vgl. auch Übungsaufgabe 14). Dann ist $\varphi(1) := (1, 0)$ nicht Eins in $\mathbb{Z} \times \mathbb{Z}$.

(vi) In Ringen besitzt jede Einheit genau ein multiplikatives Inverses, das sowohl Links- als auch Rechtsinverses ist.
Denn: Nach der Definition der Einheit u existieren $a, b \in R$ mit $au = 1$ und $ub = 1$, also gilt $b = (au)b = a(ub) = a$. Mithin ist in R jedes Linksinverse von u gleich jedem Rechtsinversen. Also existiert genau ein multiplikatives Inverses von u.

2.19 Definitionen : Ein kommutativer Ring R heißt **euklidisch**, wenn

(i) R **nullteilerfrei** ist, d.h. wenn $(ab = 0 \to a = 0 \vee b = 0)$ gilt, und es eine Abbildung $N : R \setminus \{0\} \to \mathbb{N} \cup \{0\}$ gibt so, daß

(ii) $a|b \wedge b \neq 0 \to N(a) \leq N(b)$ und

(iii) $\displaystyle\bigwedge_{a,b \in R, b \neq 0} \bigvee_{q,r \in R} (a = bq + r \wedge (r = 0 \vee N(r) < N(b)))$
(**Divisionsalgorithmus**)

gilt. Ein Element a eines kommutativen, nullteilerfreien Ringes mit 1 heißt ein **Teiler** von b, geschrieben $a|b$, wenn $\exists c \in R : b = ac$.
Sei $q \in R, q \neq 0$, q sei keine Einheit. Dann heißt q ein **irreduzibles Element**

, wenn q nur die trivialen Teiler besitzt (d.h. die Einheiten und die Produkte aus einer Einheit und q).

2.20 Bemerkungen :

(i) Die Eigenschaft (iii) von 2.19 formuliert die schon aus der Elementarschule für ganzrationale Zahlen bekannte Division mit Rest. Hierbei ist $N(z) := |z|$. Euklidische Ringe sind also im wesentlichen solche Ringe, in denen sich die Division mit Rest sinnvoll erklären läßt. Ein weiteres, auch aus der Schule bekanntes Beispiel (Polynomdivision) ist $\mathbb{Q}[x]$ (später auch $\mathbb{R}[x]$, $\mathbb{C}[x]$). $\mathbb{Q}[x]$ ist bezüglich $N(P) :=$ Grad P ein euklidischer Ring, wobei der **Grad** eines Polynoms $a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$ mit $a_n \neq 0$ zu n definiert ist.

(ii) Die Irreduzibilität verallgemeinert die Eigenschaft, die Primzahlen kennzeichnet. Also sind die irreduziblen Elemente von $\mathbb{Z}$ die Elemente $\pm p$, wobei p eine Primzahl ist. Die irreduziblen Elemente von $\mathbb{Q}[x]$ sind die linearen Polynome und gewisse quadratische Polynome, z.B. $x^2 + 1$.

(iii) Euklidische Ringe sind **Gaußsche Ringe**, d.h. es gilt die (bis auf Reihenfolge und Einheitenfaktoren) eindeutige Zerlegung in irreduzible Elemente. Z.B. $z = \pm \prod\limits_{i=1,\ldots,n} p_i^{e_i}$ in $\mathbb{Z}$ (p_i Primzahlen, $e_i \in \mathbb{N}$), $f(x) = r \prod(x + c_i) \prod(x^2 + a_j x + b_j)$ in $R[x]$. (Beweis bei Th.W. Hungerford, Algebra, Ch. III, Theorem 3.9)

2.21 Definitionen : Sei R ein kommutativer, nullteilerfreier Ring mit 1, ein sogenannter **Integritätsbereich**. $d \in R$ heißt ein **größter gemeinsamer Teiler** von $a_1, a_2, \ldots, a_n \in R$, geschrieben $(a_1, a_2, \ldots, a_n)$, wenn $(d|a_i$ für alle $i = 1, \ldots, n \wedge \{t|a_i$ für alle $i = 1, \ldots, n \to t|d\})$ gilt.

2.22 Satz : In euklidischen Ringen gilt der **Hauptsatz vom ggT**, nämlich

(i) Zu $a_1, a_2, \ldots, a_n \in R$ existiert stets ein bis auf Einheitenfaktoren eindeutig bestimmter ggT $(a_1, a_2, \ldots, a_n)$.

(ii) Es ist $(a_1, a_2, \ldots, a_n)$ als $\sum\limits_{i=1}^{n} c_i a_i$ mit $c_i \in R$ darstellbar.

Beweis: Der Beweis erfolgt mittels des sog. **euklidischen Algorithmus** (aus dem 7. Buch der Elemente des griechischen Mathematikers Euklid, der um 300 v.u.Z. in Alexandria lebte). Heute ist die Implementierung dieses Algorithmus meist eine der ersten Übungen beim Programmieren.

Wir zeigen die Aussage für $n = 2$: Wiederholte Anwendung von 2.19 (iii) ergibt:
$a_1 = q_1 a_2 + r_1$ mit $N(r_1) < N(a_2)$
$a_2 = q_2 r_1 + r_2$ mit $N(r_2) < N(r_1)$
$r_1 = q_3 r_2 + r_3$ mit $N(r_3) < N(r_2)$
...
$r_{m-1} = q_{m+1} r_m + r_{m+1}$ mit $N(r_{m+1}) < N(r_m)$
$r_m = q_{m+2} r_{m+1}$

Euklid
Aus Elements,ed. A. Tacquet, 1765

Das Verfahren muß irgendwann mit $r_{m+2} = 0$ abbrechen, da wir eine absteigende Kette $N(a_2) > N(r_1) > N(r_2) > \dots$ in $\mathbb{N}$ vorliegen haben (wegen der sog. Wohlordnungseigenschaft von $\mathbb{N}$). Verfolgen wir das Gleichungssystem von unten nach oben, so erhalten wir: r_{m+1} ist ein Teiler von r_m und wegen der zweitletzten Gleichung auch von r_{m-1} usf. aufwärts, bis wir oben folgern: $r_m | a_1 \wedge r_m | a_2$. Gehen wir von oben nach unten, so überzeugen wir uns davon, daß jeder gemeinsame Teiler von a_1 und a_2 auch ein Teiler von r_{m+1} ist. Also ist r_{m+1} ein größter gemeinsamer Teiler von a_1 und a_2.

Durch schrittweises Einsetzen – von unten nach oben gehend – ergibt sich auch der Beweis von (ii). Die Eindeutigkeit des ggT (bis auf Einheitenfaktoren): Seien d_1, d_2 zwei ggT von a_1, a_2. Dann gilt: $d_1 | d_2 \wedge d_2 | d_1$, und somit $d_1 = d_2' d_2 \wedge d_2 = d_1' d_1$. Also $d_1 = d_2' d_1' d_1$. Mithin gilt $d_2' d_1' = 1$. Daher ist d_1' eine Einheit und es ist $d_2 = d_1' d_1$.

2.23 Definitionen : $\mathbb{Z}_n^* := \{a : a \in \mathbb{Z}_n \wedge (a, n) = 1\}$ heißt **Gruppe der primen Restklassen** modulo n; denn für $(a, b) = 1$ sagen wir: a ist **prim** (oder **teilerfremd**) zu b. $\varphi(n) := |\mathbb{Z}_n^*|$ definiert die sogenannte **Eulersche φ-Funktion** , eine Abbildung $\mathbb{N} \to \mathbb{N}$.

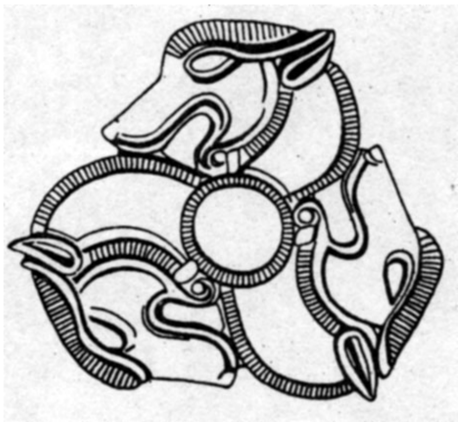
2.24 Bemerkungen :

(i) $(\mathbb{Z}_n^*, \cdot)$ ist eine Gruppe.
Denn: Wenn $(a, n) = 1$ ist, so existieren $r, s \in \mathbb{Z}$ mit $ra + sn = 1$ (2.22 (ii)). Also ist $ra \equiv 1 \mod n$, mithin hat $\widehat{a}$ ein Inverses, nämlich $\widehat{r} \in \mathbb{Z}_n$. Die übrigen Gruppenaxiome sind ebenfalls erfüllt.

(ii) Sei p eine Primzahl. Es gilt: $\varphi(p^n) = p^n - p^{n-1}$ für $n \in \mathbb{N}$.
Denn: Zu p^n nicht teilerfremd sind genau die folgenden natürlichen Zahlen $\leq p^n$: $0, p, 2p, 3p, \dots, (p^{n-1}-1)p$, also p^{n-1} Stück.

(iii) $(a,b) = 1, (a,b \in \mathbb{N}) \to \varphi(ab) = \varphi(a)\varphi(b)$.

2.25 Kleiner Fermatscher Satz :
$(a,n) = 1, (a,n \in \mathbb{N}) \to a^{\varphi(n)} \equiv 1 \mod n$.
Beweis: Wir betrachten die Menge $\langle \widehat{a} \rangle := \{\widehat{a}, \widehat{a}\widehat{a} =: \widehat{a}^2, \widehat{a}^3, \dots\}$ in $\mathbb{Z}_n^*$. Die Folge der $\widehat{a}$-Potenzen in dieser Menge endet mit $\widehat{a}^m = e$ (Begründung analog zu Zeile 1 von S. 38). Es ist $\langle \widehat{a} \rangle$ eine Untergruppe von $\mathbb{Z}_n^*$ der Ordnung m, eine sog. **zyklische, von $\hat{a}$ erzeugte** Gruppe, also nach 2.12 gilt $m|\varphi(n)$. Daher ist $\widehat{a}^{\varphi(n)} = e$, und mithin gilt die Behauptung. □

Zyklische Drehgruppen der Ordnung 4 bzw. 3 bei thrakischen Wirbelmotiven. Schmuckplatten aus dem 4. Jh. v. u. Z., Craiova, Rumänien.

Der kleine Fermatsche Satz findet mannigfache, für Informatiker interessante Antwendungen, z.B. beim probabilistischen Primzahltest nach Miller-Rabin, besonders aber beim RSA-Verfahren in der Kryptographie. Letzteres ist von den heute bekannten Verschlüsselungsverfahren das sicherste. Die Einführung von Falltür-Krypto-Systemen mit öffentlichen Schlüsseln wurde 1976 von Whitfield Diffie und Martin Hellmann vorgeschlagen (New Directions in Cryptography, IEEE Trans. Inform. Theory 22, 644). Ausgenutzt wird die Tatsache, dass es keine hinreichend schnellen Verfahren für das Ziehen von Wurzeln in $\mathbb{Z}_n$ gibt.

Wenn wir mit T den ASCII-Wert des zu verschlüsselnden Buchstaben und mit C den des verschlüsselten Buchstaben bezeichnen, so erfolgt die Verschlüsselung durch $C \equiv T^e \mod n$, wobei e und n öffentlich gemacht und so gewählt werden, dass $(e, \varphi(n)) = 1$ gilt. Dann lässt sich nämlich $ed \equiv 1 \mod \varphi(n)$ lösen, und das d ist der Entschlüsselungsexponent: $C^d \equiv T^{ed} = T^{k\varphi(n)+1} = T(T^{\varphi(n)})^k \mod n$. Wenn $(n,T) = 1$ ist, so gilt nach 2.25 $T^{\varphi(n)} \equiv 1 \mod n$ und somit $C^d \equiv T \mod n$.[4]

Diese Idee wurde von **R**ivest, **S**hamir und **A**dleman weiterentwickelt zu dem Verfahren, das heute RSA-Verschlüsselungsmethode genannt wird (Comm. ACM 21 (1978), 120 ff.): Wenn nämlich n speziell als $n = pq$ mit Primzahlen p, q, $p \neq q$, gewählt wird, so gilt $C^d \equiv T \mod n$ für jedes T. Denn im Falle von $(T, n) \neq 1$ ist $(T, n) = p$ oder $= q$, etwa $= p$. Dann ist $(T, q) = 1$ und daher $T^{\varphi(q)} \equiv 1 \mod q$. Da $p|T$, ist $n = pq|T(T^{k\varphi(q)\varphi(p)} - 1)$ für alle k und mithin wieder $T^{k\varphi(n)+1} \equiv T \mod n$ für alle k.

Ohne Kenntnis der Faktorisierung von n läßt sich $\varphi(n)$ und damit der geheim gehaltene Schlüssel d nicht hinreichend schnell ermitteln. Darin liegt die Sicherheit des Verfahrens. Der Bedarf an leicht zu handhabenden, einbruchsicheren Codes ist in den heutigen Zeiten der globalen Vernetzung enorm: z.B. für Online-Bank- oder Kauf-Geschäfte, für sichere Übermittlung von internen Betriebsdaten etc. Nach jetzigem Stand der Technik gelten Primzahlen mit 200 Dezimalstellen als sicher. Wenn stärkere Prozessoren entwickelt werden, kann man diese Marge unschwer erhöhen.

P. de Fermat

Bevor wir das Thema Ringe verlassen, wollen wir noch eine leichte, aber praktisch bedeutsame Anwendung des Rechnens im Restklassenring $\mathbb{Z}_n$ behandeln, nämlich das Prüfziffernverfahren bei der ISBN (**I**nternationale-**S**tandard-**B**uch-**N**ummer). Eine solche besteht aus 10 Ziffern, die in 4 Abschnitte gegliedert sind: Der erste Abschnitt kennzeichnet das Land (USA 0, Deutschland 3, ...), der zweite den Verlag, der dritte das Buch, und der vierte besteht aus der Prüfziffer $z_{10} \equiv \sum_{i=1}^{9} i z_i \mod 11$ (für den Rest 10 wird X geschrieben). Zum Beispiel hat das bekannte Buch von Donald E. Knuth: The Art of Computer Programming, vol. 3, Sorting and Searching, die ISBN 0-201-03803-X. Das Prüfverfahren erkennt alle Einzelfehler und Doppelfehler bis auf einen Teil der Zwillingsvertauschungen und phonetischen Fehler.

[4]Bei konkreten Implementationen des Verfahrens werden nicht die ASCII-Werte einzelner Textbuchstaben sondern Blöcke aus solchen potenziert. Die Blocklänge wird z. B. einheitlich so gewählt, dass die Zahlenwerte der Blöcke gering unterhalb des Schlüssels n liegen.

Noch besser ist die Prüfbedingung $\sum_{i=1}^{n} 2^{i-1} z_i \equiv 0 \mod 11$. Damit arbeitet angeblich die Dresdner Bank.

Zum Abschluß empfehlen wir noch den

Slogan: Der Kongruenz $\mod n$ in $\mathbb{Z}$ entspricht die Gleichheit in $\mathbb{Z}_n$.

2.26 Definitionen : Ein kommutativer Ring K mit $1 \neq 0$ heißt ein **Körper**, wenn $K^* := K \setminus \{0\}$ aus Einheiten besteht. Ein endlicher Körper wird auch **Galoisfeld** genannt.

2.27 Beispiele :

(i) Die Menge $\mathbb{Q}$ der rationalen Zahlen ist bezüglich der Addition und Multiplikation ein Körper. Das Gleiche stellen wir im Vorgriff von der Menge $\mathbb{R}$ der reellen Zahlen fest .[5]

(ii) Wenn p eine Primzahl ist, so ist $\mathbb{Z}_p$ ein Galoisfeld der Ordnung p.
Denn: Nach 2.24 (ii) ist $|\mathbb{Z}_p^*| = p - 1$ und daher $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$. Wegen 2.24 (i) besteht also $\mathbb{Z}_p \setminus \{0\}$ aus lauter Einheiten.

(iii) Auf der Menge $\mathbb{R}^2$ definieren wir folgendermaßen eine Addition und eine Multiplikation: $(a, b) + (c, d) := (a + c, b + d)$, $(a, b) \cdot (c, d) := (ac - bd, ad + bc)$.

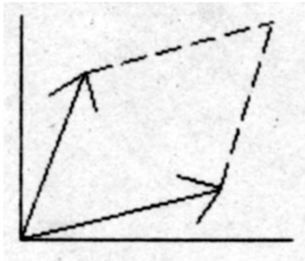
Es ist leicht nachzuprüfen, dass $(\mathbb{R}^2, +, \cdot)$ ein Körper ist, der sogenannte **Körper $\mathbb{C}$ der komplexen Zahlen**.

Statt mit Zahlenpaaren (a, b) wird gewöhnlich mit Ausdrücken der Form $a + ib$ gearbeitet, also in dem durch den Körperisomorphismus $(a, b) \mapsto a + ib$, $(a, 0) \mapsto a$, $(0, 1) \mapsto i = 1 \cdot i$ festgelegten Bild, das ebenfalls mit $\mathbb{C}$ bezeichnet wird.

Es ist $(0, 1) \cdot (0, 1) = (-1, 0)$, also $i^2 = -1$. Sei $z := a + ib \in \mathbb{C}$. $\overline{z} := a - ib$ heißt die zu z **konjugiert-komplexe Zahl** (oder die **Konjugierte** von z). $\operatorname{Re} z := a$ heißt der **Realteil** von z, $\operatorname{Im} z := b$ der **Imaginärteil** von z.

[5] Während sich der Körper $\mathbb{Q}$ als Menge der Brüche aus dem Ring $\mathbb{Z}$ leicht konstruieren lässt, werden zur Konstruktion von $\mathbb{R}$ über die algebraischen Methoden hinaus zusätzlich analytisch-topologische Hilfsmittel benötigt, die von unserer Systematik her in das dritte Kapitel gehören. Es sei uns aber gestattet, $\mathbb{R}$ bereits hier (wie auch im Beispiel zu 1.10) in naiver Weise für Beispiele zu gebrauchen.

Wenn die Elemente von $\mathbb{C}$ gemäß dem Beispiel von Seite 24 unten als Punkte in einem rechtwinkligen, rechtshändigen Cartesischen Koordinatensystem dargestellt werden – man spricht dann auch von der Darstellung in der **Gaußschen Ebene**, die horizontal verlaufende Achse wird **reelle**, die vertikale **imaginäre Achse** genannt –, so ergibt sich eine anschauliche Darstellung der Addition komplexer Zahlen, wie in nebenstehender Figur gezeigt.



Addition in $\mathbb{C}$

Diese Situation müsste aus der Physik von der Addition der Kräfte (im sog. Kräfteparallelogramm) her bekannt sein. Der Übergang zum konjugiert komplexen Wert bedeutet in diesem Kontext eine Spiegelung an der reellen Achse. Die geometrische Veranschaulichung der Multiplikation im Komplexen erfolgt am Ende des fünften Kapitels.

In $\mathbb{C}$ gelten die Beziehungen $\overline{\overline{z}} = z$; $z\overline{z} = (a+ib)(a-ib) = a^2+b^2 = |z|^2$, wobei $|z| := \sqrt{(\operatorname{Re} z)^2 + (\operatorname{Im} z)^2}$ der sogenannte **Betrag** von z ist, der der Länge des „Vektors“ z entspricht; $z + \overline{z} = 2 \operatorname{Re} z$; $z - \overline{z} = 2i \operatorname{Im} z$.

2.28 Satz : Zu jeder Primzahl p und jedem $n \in \mathbb{N}$ existiert (bis auf Isomorphie) genau ein Galoisfeld von p^n Elementen, bezeichnet mit $\mathbb{F}_{p^n}$. Damit sind alle endlichen Körper aufgezählt. Der kleinste Teilkörper (sog. **Primkörper**) von $\mathbb{F}_{p^n}$ ist isomorph zu $\mathbb{Z}_p$.
Ein Beweis dieses Satzes findet sich in jedem Lehrbuch der Algebra. Endliche Körper sind für Informatiker z.B. im Kontext der Codierungstheorie interessant.

2.29 Definitionen : Ein Körper K heißt **angeordnet**, wenn es $P \subset K^*$ so gibt, dass

(i) $\bigwedge\limits_{x \in K^*} x \in P \sqcup -x \in P$ und

(ii) $\bigwedge\limits_{a,b \in P} (a + b \in P \wedge ab \in P)$ gilt.

Dann heißen P **Positivitätsbereich**, seine Elemente **positiv** und die Elemente von $-P := \{x : -x \in P\}$ **negativ**. Wir schreiben $a < b$, wenn $b - a \in P$ gilt.

2.30 Definitionen : Eine Relation ρ auf einer Menge M heißt eine **Ordnung** auf M, wenn sie reflexiv, transitiv und **antisymmetrisch** (d.h.

$x\rho y \wedge y\rho x \to x = y$) ist. Eine Ordnung heißt **linear**, wenn $\bigwedge\limits_{x,y\in M} x\rho y \vee y\rho x$ gilt. Eine linear geordnete Menge heißt auch **Kette**.

2.31 Beispiele :

(i) Die natürliche Ordnung $\leq$ auf der Menge $\mathbb{N}$ ist linear. Die Teilbarkeitsrelation auf $\mathbb{N}$ ist eine nichtlineare Ordnung.

(ii) Die Inklusion $\subset$ ordnet Potenzmengen (i.a. nichtlinear).

(iii) Die Menge $\mathbb{R}$ ist bezüglich der natürlichen Ordnung linear geordnet und bezüglich der Menge $P := \mathbb{R}^+ := \{x \in \mathbb{R} : x > 0,\ >$ ist die natürliche Ordnung$\}$ angeordnet.

Achtung: Beachten Sie den Unterschied zwischen den Begriffen Ordnung und Anordnung![6]

2.32 Bemerkungen : Sei K angeordnet mit Positivitätsbereich P. Dann gilt:

(i) $x \in K^* := K \setminus \{0\} \to x^2 \in P$
Denn: In Körpern gilt $(-1)(-1) = 1$, da $0 = (-1)\cdot 0 = (-1)(-1+1) = (-1)(-1) + (-1)\cdot 1 = (-1)(-1) + (-1)$ gilt, $(-1)(-1)$ also das additive Inverse von -1 ist. Mithin gilt auch für $-x \in P$ $x^2 = (-x)^2 \in P$ ist.

(ii) $1 \in P$, $n \cdot 1 \in P$ für alle $n \in \mathbb{N}$.
Denn: Da nach 2.26 im Körper $1 \neq 0$ ist, gilt $1 \in P \ \vee\ 1 \in -P$. Die Annahme $-1 \in P$ führt nach (i) und nach $(-1)(-1) = 1$ auf den Widerspruch $1 \in P \cap -P$.

(iii) K ist die disjunkte Vereinigung von P, $-P$ und 0

(iv) Durch $b - a \in P \leftrightarrow: a < b$ wird eine lineare Ordnung $\leq$ der Menge K induziert mit den folgenden Eigenschaften:

$$x > 0 \ \wedge\ xy > 0 \ \to\ y > 0 \quad ,$$

$$x > 0 \ \to\ x^{-1} > 0 \quad ,$$

[6] Jede Menge lässt sich ordnen, nach dem Auswahlaxiom sogar wohlordnen (siehe 2.38). Aber nicht jeder Körper kann angeordnet werden (siehe 2.32 (v)).

$$0 < x < y \;\rightarrow\; 0 < y^{-1} < x^{-1} \quad .$$

Denn: Sei $y \leq 0$ angenommen. Wenn $y = 0$ ist, so ist $xy = 0$ (Widerspruch). Wenn aber $y < 0$ ist, so ist $-xy \in P$ und (nach Voraussetzung) $xy \in P$ (Widerspruch zu (iii)). Die beiden restlichen Implikationen beweisen Sie bitte übungshalber selbst!

(v) $\mathbb{C}$ kann nicht angeordnet werden, $\mathbb{F}_p$ kann nicht angeordnet werden.
Denn: Es müsste sonst in $\mathbb{C}$ wegen (i) $i^2 \in P$ gelten. Nun ist aber $-1 \notin P$! In $\mathbb{F}_p$ gilt $p \cdot 1 = 0$, aber nach (ii) wäre $p \cdot 1 \in P$ (Widerspruch!).

2.33 Definitionen : Es seien K ein Körper, $\overline{K}$ ein angeordneter Körper mit Positivitätsbereich $\overline{P}$ (z.B. $\mathbb{R}$ angeordnet bezüglich der natürlichen Ordnung $\leq$). Eine Abbildung $|\ | : K \rightarrow \overline{P} \cup \{0\}$ heißt ein **Absolutbetrag** auf K, wenn

(i) $|x| = 0 \leftrightarrow x = 0 \quad ,$

(ii) $|xy| = |x||y| \quad$ und

(iii) $|x + y| \leq |x| + |y|$

für alle $x, y \in K$ gelten. Die Beziehung (iii) heißt **Dreiecksungleichung**.

2.34 Bemerkungen :

(i) Der in 2.27 (iii) für komplexe Zahlen definierte Betrag ist ein Absolutbetrag im Sinne der Definition in 2.33.
Denn: Eigenschaft (i) ist klar und es gilt

$$\begin{aligned} |(a+ib)(c+id)| &= \sqrt{(ac-bd)^2 + (ad+bc)^2} \\ &= \sqrt{(a^2+b^2)(c^2+d^2)} \\ &= |a+ib||c+id| \quad . \end{aligned}$$

Da $(ad - bc)^2 \geq 0$ ist, gilt $2abcd \leq a^2d^2 + b^2c^2$ und mithin $a^2c^2 + 2abcd + b^2d^2 \leq a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2$. Ziehen wir auf beiden Seiten die Quadratwurzel, so erhalten wir $ac + bd \leq \sqrt{(a^2+b^2)(c^2+d^2)}$. Daraus folgt $\sqrt{(a+c)^2 + (b+d)^2} \leq \sqrt{a^2+b^2} + \sqrt{c^2+d^2}$, also Eigenschaft (iii).

(ii) Im Dreieck ist die Summe der Länge zweier Seiten größer gleich der Länge der dritten, daher der Name „Dreiecksungleichung“ für (iii) (vgl. die Figur S.61).

(iii) $|1| = |-1| = 1$.
Denn: Wegen 2.33 (ii) gilt $|x| = |x \cdot 1| = |x| \cdot |1|$ und somit $|1| = 1$. Wenn im Körper $x^2 = 1$ gilt, also $0 = (x+1)(x-1)$, so ist wegen der Nullteilerfreiheit $x = \pm 1$.

(iv) $|x - y| \leq |x| + |y|$.
Denn: Es gilt $|x - y| = |x + (-y)| \leq |x| + |-y| = |x| + |y|$.

(v) $|x| - |y| \leq |x \pm y|$.
Denn: Mit $u := x + y$ und $v := -y$ gilt $|x| = |u + v| \leq |u| + |v| = |x + y| + |y|$, also $|x| - |y| \leq |x + y|$. Mit $u := x - y$ und $v := y$ erhalten wir analog $|x| - |y| \leq |x - y|$.

(vi) Wenn K auch angeordnet ist, so induziert die Anordnung einen Absolutbetrag mittels

$$|a| := \begin{cases} a & \text{für } a > 0 \\ 0 & \text{für } a = 0 \\ -a & \text{für } a < 0 \end{cases}$$

Denn: Prüfe die Eigenschaften (i), (ii), (iii) von 2.33 nach!

(vii) Für den nach (v) induzierten Absolutbetrag gilt $|x| - |y| \leq ||x| - |y|| \leq |x \pm y|$.
Denn: Die rechte Ungleichung folgt unmittelbar aus 2.33(iii) und 2.34(iii). Nach 2.34(iv) gilt $|x| - |y| \leq |x \pm y|$. Wenn wir hierin x und y vertauschen, so erhalten wir $-(|x| + |y|) = |y| - |x| \leq |y \pm x| = |x \pm y|$, also $||x| - |y|| \leq |x \pm y|$.

2.35 Definition : Ein angeordneter Körper K heißt **archimedisch angeordnet**, wenn das Axiom des Archimedes gilt: $\bigwedge\limits_{a,b \in K, a > 0} \bigvee\limits_{n \in \mathbb{N}} na > b$.

2.36 Bemerkungen : Die natürliche Anordnung in $\mathbb{R}$ ist archimedisch. Daher gelten dort:

(i) $\forall x \in \mathbb{R}^+ \cup \{0\}\ \exists_1 n_x \in \mathbb{N} \cup \{0\} : n_x \leq x < n_x + 1$ (Existenz von $\lfloor x \rfloor$, floor in math.h in C).
Denn: Wegen der Archimedizität von $\mathbb{R}$ kann x durch $n^* \cdot 1$ überschritten werden: $n^* \cdot 1 > x$. Nimm das kleinste solche n^*, setze $n_x := n^* - 1$ und setze fort auf $\mathbb{R}^-$.

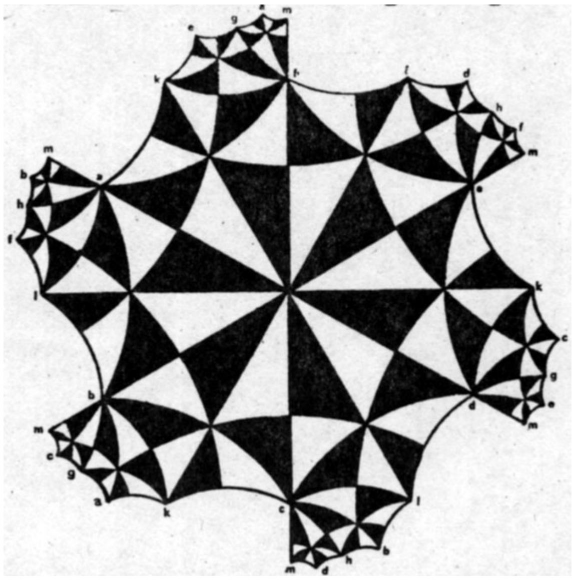
(ii) $\forall \epsilon > 0\ \exists n \in \mathbb{N} : \frac{1}{n} < \epsilon$.
Denn: $\exists n \in \mathbb{N} : n \cdot 1 > \frac{1}{\epsilon}$.

(iii) Für $x \geq -1$ und $n \in \mathbb{N}$ gilt $(1+x)^n \geq 1+nx$ (**Bernoullische Ungleichung**) .
Beweis durch vollständige Induktion: Nach Induktionsannahme und nach Voraussetzung ist $(1+x)^{n+1} \geq (1+nx)(1+x) = 1+(n+1)x+x^2 \geq 1+(n+1)x$.

Slogan: Bernoulli ist abgehackter Binomi.

(iv) $b > 1 \rightarrow$
$\forall a \in \mathbb{R}\, \exists n \in \mathbb{N} : b^n > a$.
Denn: Wir setzen $x := b-1$, und somit ist $x > 0$, also $\exists n \in \mathbb{N} : nx > a-1$ wegen der Archimedizität von $\mathbb{R}$. Also ist $b^n = (1+x)^n \geq 1+nx > a$.

(v) $0 < b < 1 \rightarrow$
$\forall \epsilon > 0\, \exists n \in \mathbb{N} : b^n < \epsilon$.
Denn: Wegen 2.32(iv) impliziert die linke Seite $b^{-1} > 1$, also existiert nach 2.36(iv) $n \in \mathbb{N}$ mit $(b^{-1})^n > \epsilon^{-1}$ und somit auch mit $b^n < \epsilon$.



Eine reguläre Pflasterung mit Drehgruppe der Ordnung 72 auf einer orientierbaren Fläche vom Geschlecht 4.

Abschließend noch einige Ausführungen zum sogenannten Auswahlaxiom.

2.37 Satz : Sei M eine geordnete Menge. Dann sind äquivalent:

(i) **Minimalbedingung**, d. h., jede nichtleere Teilmenge L von M besitzt ein (in L) minimales Element. Wir sagen dann auch, dass M **wohlgeordnet** ist.

(ii) Wenn $m_1 \geq m_2 \geq \ldots \geq m_i \geq \ldots$ eine absteigende Kette in M ist, so existiert ein $n \in \mathbb{N}$ mit $m_n = m_{n+1} = \ldots$ (sog. **Bedingung des Abbrechens absteigender Ketten**.

(iii) Sei $\mathcal{E}$ eine Eigenschaft, für die gilt:

(a) $\mathcal{E}$ gilt für alle minimalen Elemente aus M.

(b) Wenn $\mathcal{E}$ für alle Elemente gilt, die einem Element $m \in M$ streng vorangehen, so gilt $\mathcal{E}$ auch für m.

Dann gilt $\mathcal{E}$ für alle Elemente aus M (**Induktionsbedingung**).

Beweis: (i) $\longrightarrow$ (ii): Sei $m_1 \geq m_2 \geq \ldots \geq m_i \geq \ldots$ eine absteigende Kette in M. Wir betrachten die aus den Elementen dieser Kette gebildete Menge $L := \{m_1, m_2, \ldots, m_i, \ldots\}$. Sie ist nicht leer, also enthält L nach (i) ein minimales Element m_k. Wegen des Absteigens der Kette und wegen der Minimalität von m_k gilt $a_k = a_{k+1} = \ldots$.
(ii) $\longrightarrow$ (iii): $\mathcal{E}$ erfülle (iii)(a) und (b) und es gelte (ii). Sei L die Teilmenge von M aller derjenigen Elemente, für die $\mathcal{E}$ nicht gilt. Angenommen, L sei nicht leer, also $l_1 \in L$. l_1 kann wegen (iii)(a) in M nicht minimal sein, also existiert wenigstens ein strikter Vorgänger in M. Unter den strikten Vorgängern von l_1 existiert einer, der in L liegt und l_2 genannt sei. Andernfalls wäre nämlich wegen (b) $l_1 \notin L$. Argumentiere für l_2 so wie eben für l_1 und folgere einen strikten Vorgänger l_3. So fortfahrend erhalten wir eine strikt absteigende Kette $l_1 > l_2 > l_3 > \ldots$, die nicht abbricht. Also ist L leer, und $\mathcal{E}$ gilt für alle Elemente von M.
(iii) $\longrightarrow$ (i): Wir wenden das Induktionsprinzip für die Eigenschaft $\mathcal{E} :=$ "besitzt ein minimales Element "auf die Menge $\mathcal{P}(M) \setminus \emptyset$ an. Die minimalen Elemente von $(\mathcal{P}(M) \setminus \emptyset, \subset)$ sind genau die einelementigen Teilmengen. Für sie gilt die Eigenschaft $\mathcal{E}$ trivialerweise. Sei $L \in \mathcal{P}(M) \setminus \emptyset$. Wir zeigen : Wenn $\mathcal{E}$ für alle echten Teilmengen von L gilt, dann gilt es auch für L. Wählen wir nämlich $x \in L$ und setzen wir $L \setminus \{x\} =: A$, so ist x oder ein nach Induktionsannahme existierendes minimales Element von A minimal in $L = A \cup \{x\}$. Also sind (iii)(a) und (b) für $\mathcal{E}$ in $\mathcal{P}(M) \setminus \emptyset$ gültig, also gilt nach Voraussetzung (iii) $\mathcal{E}$ auf $\mathcal{P}(M) \setminus \emptyset$, also gilt (i) für M. □

2.38 Satz : Folgende Aussagen sind äquivalent:

(i) (**Auswahlaxiom**) Sei M eine Menge. Dann existiert auf $\mathcal{P}(M) \setminus \emptyset$ eine Funktion f, die jeder nichtleeren Teilmenge L von M ein Element $f(L) \in L$ zuordnet.

> **Slogan:** Das Auswahlaxiom stellt die Existenz einer Funktion sicher, welche aus jeder nichtleeren Teilmenge ein Element herausgreift.

(ii) (**Satz von Zermelo** oder **Wohlordnungssatz**) Jede Menge lässt sich wohlordnen.

(iii) (**Satz von Kuratowski-Zorn** oder **Zornsches Lemma**) Wenn jede Kette einer geordneten Menge M eine obere Schranke hat, so folgt auf jedes Element von M ein maximales Element.

Beweis: In Hewitt-Stromberg: Real and Abstract Analysis, Thm. 3.12.

2.39 Bemerkungen : Standardbeispiel für eine wohlgeordnete Menge ist $(\mathbb{N}, \leq)$, für eine nicht wohlgeordnete Menge $(\mathbb{Z}, \leq)$.
Die Verwendung des Auswahlaxioms war lange Zeit umstritten. Jedoch hat Gödel 1940 gezeigt, dass ein Axiomensystem der Mengenlehre mit Auswahlaxiom und Kontinuumshypothese relativ widerspruchsfrei zu dem genannten Axiomensystem ohne die beiden letzteren Axiome ist.