

STRUKTUREN
der

MATHEMATIK

Teil I

I gave it to U

und now it's yours
to give it to someone else

A brother to a brother

**from one to
another**

Eric Burdon

Eric Burdon & War - The Vision Of Rassan

www.youtube.com/watch?v=nV4rfZ6oN_M&list=PLaP9_vNaAUZTh_CCPJhNFv-e1EGgImP6h

Meinem Freund **Arno Fehringer** gewidmet!

In der Algebra und insbesondere in der Arithmetik – wie überhaupt überall in der gesamten Mathematik – rechnen wir mit Zahlen, die eine gewisse Struktur haben. Man spricht von einem Zahlkörper. Dieser wiederum stützt sich auf die Gruppenbegriffe, mit denen wir uns daher zunächst etwas genauer befassen. Aber keine Angst, ich werde es ihnen so einfach wie nur möglich darbieten.

Allerdings: Jedem recht getan ist eine Kunst, die niemand kann!

1	10	11	100	101	110	111	1000	1001	1010	
0	1	10	11	100	101	110	111	1000	1001	
-1	0	1	10	11	100	101	110	111	1000	
-10	-1	0	1	10	11	100	101	110	111	
-11	-10	-1	0	1	10	11	100	101	110	111
-100	-11	-10	-1	0	1	10	11	100	101	110
-101	-100	-11	-10	-1	0	1	10	11	100	101
-110	-101	-100	-11	-10	-1	0	1	10	11	
	-110	-101	-100	-11	-10	-1	0	1	10	
usw.		-110	-101	-100	-11	-10	-1	0	1	
			-110	-101	-100	-11	-10	1	0	

Verknüpfungstafel fürs Plus in Dualzahl-Darstellung (Zweiersystem)

Die **Addition** bildet in der Menge der ganzen Zahlen **eine kommutative Gruppe**, die zyklisch ist. Dazu ist eine Erweiterung der natürlichen Zahlen durch die negativen Gegenzahlen notwendig!
Die neutralen Null-Elemente (graublau) liegen auf der 2. Winkelhalbierenden

Die Mutter aller Zahlen sind die natürlichen Zahlen bzw. die Gruppe Z der ganzen Zahlen bezüglich der Addition. Da man diese durch das Ab-Zählen, d.h. durch die ständige Addition um Eins, erzeugen kann, spricht man von der **zyklischen Gruppe C_∞** , die auch kommutativ ist (d.h. die Summanden sind vertauschbar). Die Summe zweier ganzen Zahlen ergibt wiederum eine ganze Zahl (man spricht von der Abgeschlossenheit in Z). Ferner spielt die Reihenfolge was man bei mehreren Summanden zuerst addiert, keine Rolle (Assoziativität). Ferner gibt es eine ganz besondere Zahl, für welche die Menschheit ganz früher lange kein Zeichen hatte, nämlich dem Vertreter für das Nichts, sprich die Null. Diese ändert nichts am Wert der Summe, wenn sie addiert wird (man spricht vom NEUTRALEN Element). Schließlich gibt es zu jeder ganzen Zahl eine Gegenzahl (man spricht vom INVERSEN Element), welche die Zahl neutralisiert, so daß die Summe von Zahl und ihrer Gegenzahl verschwindet, also zum neutralen Element Null wird. Allerdings hat es wiederum relativ lange gedauert, bis negative Zahlen, die ja kleiner als Null sind, als Zahlen anerkannt wurden: Sogar der Begründer der Koordinatengeometrie, Rene Descartes (1596-1650), verweigerte ihnen noch das Existenzrecht!

Was ist nun eine abstrakte **Gruppe**struktur?

Die (vier) Gruppengesetze !

1.) Abgeschlossenheitsgesetz:

Die Operation bringt als Ergebnis stets einen Wert, der in der Menge liegt

2.) Es gilt das Assoziativgesetz

$$(a + b) + c = a + (b + c) \quad (a * b) * c = a * (b * c)$$

Aber das Potenzieren ist **nicht** assoziativ zB. $9(9^9) \neq (9^9)^9 = 9^{81}$

3.) Es gibt ein sog **neutrales Element**, mit deren Verknüpfung nichts geschieht:

Bei der Addition ist es die Null¹, weil $a+0 = 0$ ist,
bei der Multiplikation ist es die Eins!

4.) **Zu jedem Element** existiert **ein Umkehrelement** (**inverses Element**), das dieses neutralisiert, d.h. zum neutralen Element macht.

Ein Element kann auch zugleich sein eigener Gegenpart (zu sich selbst invers) sein

Beispiel eine gerade Zahl g : wegen $g+g = g$ (für ungerade u ist $u+u = g$)

Bei der Addition in der unendlichen Zahlenmenge Z ist es die Gegenzahl,
die mit einem Minus gekennzeichnete
entsprechende negative Größe:

$$a + (-a) = 0 \text{ neutrales Element}$$

Bei der Multiplikation ist das Inverse der Kehrwert, denn $a * a^{-1} = 1$

Zudem gilt **für kommutative Gruppen** (wenn die Diagonale Symmetrieachse ist) noch das **Vertauschungsgesetz** $a+b = b+a$

$$a * b = b * a$$

¹ Gegenbeispiel: Das Potenzieren ist nicht vertauschbar $a^b \neq b^a$

Die Gruppenstruktur sichert die eindeutige Auflösbarkeit von Gleichungen.

Wie beim Sudoku kommt in der Gruppen-Verknüpfung jedes Element genau einmal in jeder Zeile und jeder Spalte vor².

Denn wäre in einer Zeile ein Element doppelt vorhanden, so wäre das Ergebnis zweier Verknüpfungen, etwa mit b und mit c , gleich.

Aus $a \circ b = a \circ c$ folgt aber, wenn man die Gleichung mit dem Inversen a^{-1} von a verknüpft, dass $a^{-1} \circ a \circ b = a^{-1} \circ a \circ c$

also in Wahrheit $b = c$ ist.

Analoges gilt für die Spalten: Wären zwei Spaltenelemente gleich, etwa

$$a \circ c = b \circ c$$

dann folgt mit $a \circ c \circ c^{-1} = b \circ c \circ c^{-1}$, dass $a = b$ ist.

Wann sind nun zwei Gruppen gleich?

Gruppen sind strukturell gleich, wenn sie operationstreu sind, d. h. es besteht ein Isomorphismus (oder Gruppen-Homomorphismus) zwischen den

Gruppen:

$$\varphi(a \square b) = \varphi(a) \diamond \varphi(b)$$

(\square und \diamond sind die beiden Gruppenverknüpfungen)

² Beim Sudoku (su ist japanisch und heißt Zahl, doku = einzig, einsam) kommt zudem jede Ziffer $\neq 0$ des 9x9-Quadrats (und auch sogar in den neun 3x3-Quadraten) einmalig vor. **Mit nur 16 Vorgaben kann man aber das Sudoku nicht mehr eindeutig lösen**, wie mit Hilfe eines Computers, der fast an Jahr rechnete, bewiesen wurde.

→ Spektrum der Wissenschaften April 2010

Machen wir nun noch einen kurzen Ausflug zur Gruppentheorie und Geometrie!

*(insbesondere zuerst zur Planimetrie als ein Modell der
Zahlenarithmetik und Algebra von Q^2 oder R^2)*

In der analytischen Geometrie interpretiert man nun die algebraische Strukturiertheit des unendlichen Zahlkörpers R der reellen Zahlen. Bei der Rechenoperationen 1. Stufe bildet die Addition – wie gesagt- eine **unendliche zyklischen Gruppe** (alle Elemente sind aus einem Element erzeugbar, nämlich aus der Einheit 1). Und auch die Rechenoperation 2. Stufe, die Multiplikation, bildet in R eine kommutative Gruppe (sofern man das additive Element heraus nimmt³). Die beiden Gruppen bilden mit dem sie verbindenden Distributivgesetz $a*(b+c) = a*b + a*c$ den **Zahlen-Körper $(R; +, *)$** .

Für die Ebene bildet man die Menge $R \times R$, die Menge der Zahlenpaare R^2 , die nun die Punkte der Ebene sind. Man kann stattdessen dazu auch die „eindimensionale“ Menge der komplexen Zahlen C verwenden (Gaußsche Zahlenebene), denn $C(+, *)$ ist auch ein kommutativer Körper. Mit der Differenz zweier Zahlenpaare (von zwei Punkten A und B) kann man nun **Vektoren** über einem Vektorraum VR bilden, die ebenfalls bezüglich der Addition eine Gruppe bilden, wie auch die

³ Das Inverses Element zur Null wäre die Pseudozahl $\gg\infty<$, weil $1/\infty = 0$ ist

2 x2 **Matrizen M** zB. speziell für mit der Determinante $\text{Det } M = 1$ sind es die flächeninvarianten linearen Abbildungen in der Ebene, mit fixem Ursprung:

$$(x', y') = \mathbf{M} (x, y) \quad \text{mit der Determinante } \text{Det } M = 1$$

Abbildungen, die den Ursprung $(0, 0)$ fest lassen,

$$\text{also } \mathbf{M} \text{ mal Vektor } (0, 0) = (0, 0)$$

Die **Matrizenmultiplikation** ist aber **nicht kommutativ**

(nicht mehr vertauschbar):

$$A*B \neq B*A$$

da die Reihenfolge bzw. die Hintereinander Ausführung der Abbildungen verschiedene Ergebnisse liefern kann. Beispielsweise liefert eine zuerst ausgeführte Achsenspiegelung (Klappung) um die erste Winkelhalbierende $y=x$ mit hintereinander ausgeführter anschließender Drehung um den Ursprung mit 30° ein anderes Bild, als wenn zuerst um 30° gedreht und dann an $y=x$ gespiegelt wird.

Die Matrizen $(M, +, *)$ bilden keinen Körper, sondern wegen der multiplikativen Halbgruppe nur eine Ringstruktur.

Die euklidische Ebene kann man auch als ein Modell unseres unendlichen Zahlenkörpers der rationalen \mathbb{Q}^2 oder reellen Zahlen \mathbb{R}^2 interpretieren. Insbesondere können wir über endlich Gruppen bzw. endliche Zahlen-Körper⁴ **endliche euklidische Geometrien** erzeugen! Genau das wollen wir nun demonstrieren.

⁴ Jede multiplikative Gruppe eines endlichen Körpers ist auch stets zyklisch und daher ist jeder endliche Körper auch kommutativ. Die Restklassen modulo einer Primzahl sind immer kommutative Körper. Man kann auch beweisen, daß zu jeder Primzahlpotenz p bis auf Isomorphie **genau einen Körper** gibt.

Da die Unendlichkeit immer schwer zu handhaben ist, da man kann ja nie „zu einem Ende“ kommt, wollen wir uns einmal vorstellen, daß eine Gerade nicht unendlich viele Punkte hätte, sondern jede Geraden soll nur aus n Punkten bestehen! Und wenn wir das nun ganz extrem auf die Spitze treiben wollen, dann müssen es mindestens zwei Punkte sein. Wir verwenden daher einen Zahlenkörper mit nur zwei Elementen, nämlich der Null und der Eins, der kleinsten endlichen Gruppe!

Die aller kleinste ist die **Modulo-Zahlengruppen** $\text{mod } 2$, die **Restklassenzahlen** bei der Teilbarkeit durch 2. Bei der Teilung durch zwei entweder der *Rest 0 für gerade Zahlen* oder den *Rest 1 für ungerade Zahlen*, und somit existieren nur die beiden Restklassenzahlen Nullquer und Einsquer (zur Unterscheidung von der Eins schreibe ich manchmal auch I dafür). Diese beiden bilden bezüglich der Addition die überhaupt kleinste-mögliche Gruppe:

Gerade plus gerade gibt ebenso wieder **gerade** wie **ungerade+ungerade**, (sonst ungerade); analog zu den Vorzeichen bei der Multiplikation: Nur gleiche Vorzeichen der beiden Faktoren ergeben + (sonst minus)

Verknüpfungstafel

plus	0	I
0	0	I
I	I	0

0 ist neutral

bezüglich des Addierens

(Vorzeichen + und -)

mal	1	-1
1	1	-1
-1	-1	1

1 ist neutral

bezüglich des Multiplizierens

Was noch etwas schwer zu verdauen ist, bei diesen endlichen Gruppen:

Nicht nur die Addition von nur Nullen ergibt Null, sondern hier bei Modulo zwei ist

$$I + I = 0$$

Es ist eben wie bei der Uhr, nach 12 kommt nicht 13, sondern die Ziffer 1!

Bevor wir hiermit weitermachen, noch ein kurzer Hinweis bezüglich Null hoch Null!

Erst in der **Strukturmathematik** erkennt man für endliche Gruppen die herausragende Bedeutung **der Nichtigkeit (0) und der Einheit (1)**. Denn diese grundlegende Einzigartigkeit dieser beiden Zahlen kann nirgends besser verstanden werden als bei den algebraischen Zahlen-Strukturuntersuchungen von endlichen Gruppen:

Während 1 mal 1 ebenso wie 1 hoch 1 stets immer 1 ist,
bleibt die Frage was Null hoch Null ist?

In allen endlichen Restklassen-Zahlen-Gruppen ist $0^0 = 0$ Null, aber bei den unendlichen Zahlengruppen, mit denen wir immer rechnen, ist $0^0 = 1$ also nicht null, sondern etwas, nämlich Eins! **Nichts mit Nichts potenziert erzeugt etwas, nämlich die Eins!**

hoch	0	1	128	2187	16384	78125	279936	823543
6	0	1	64	729	4096	15625	46656	117649
5	0	1	32	243	1024	3125	7776	16807
4	0	1	16	81	256	625	1296	2401
3	0	1	8	27	64	125	216	343
2	0	1	4	9	16	25	36	49
1	0	1	2	3	4	5	6	7
0	?	1	2	3	4	5	6	7

Verknüpfungstafel fürs Potenzieren (ist keine Gruppe)

Hier ist keine Symmetrie zur 1. Winkelhalbierenden mehr vorhanden,
da das **Potenzieren weder kommutativ noch assoziativ** ist!

Auch die **Multiplikation** bildet - aber in der Menge der **rationalen Zahlen** ohne die Null (= das neutrale Element der Addition) eine kommutative Gruppe, die **dieselbe Struktur** hat! Ob sie auch zyklisch ist)?

Auch auf die Gefahr hin, mich zu wiederholen:

Die ultimativ **kleinste Gruppe** (bzw. der kleinste denkbare Zahlenkörper) besteht also aus genau **zwei** Zahlen, etwa 0 und 1. Die Elemente müssen aber keine Ziffern sein.

An Stelle der Ziffern oder Zahlen können wir aber auch andere Symbole verwenden!

Schreiben wir zB. anstatt **Null g** (wie gerade)

und statt **Eins u** (wie ungerade; was den Rest 1 bei der Teilung durch 2 liefert),

oder bei der Multiplikation **+** für positives Vorzeichen und an Stelle der Minuszahlen

- für die Negativität, dann haben wir dieselbe Struktur.

Plus	g	u
g	g	u
u	u	g

g ist neutral

Multiplikation	+	-
+	+	-
-	-	+

+ ist neutrales Element

g sei eine **gerade Zahl** und **u** eine **ungerade Zahl**. Die Summe einer geraden Zahl und einer geraden ist wiederum gerade, aber auch zwei ungerade Zahlen addiert sind zu einer geraden (während das Produkt zweier ungeraden Zahlen aber immer ungerade ist)

Entsprechend ergibt plus mal plus wieder plus und aber auch eine negative Zahl mit einer negativen multipliziert wird positiv:

$$n \text{ mal } n = p \quad \text{oder} \quad \boxed{- * - = +}$$

(sonst gäbe es keine komplexen Zahlen, wo ja die imaginäre Einheit $i = \sqrt{-1}$ ist.)

Nur bei verschiedenen Vorzeichen erhält man als Produkt etwas Negatives

(n = negatives Vorzeichen). Das eine (positive) Element ist das neutrale Element und das andere (negative) ist zu sich selbst invers.

Natürlich gibt es noch viele weitere Beispiele für diese minimalste Gruppe, wie etwa das Ein- oder Aus-Schalten einer Glühbirne oder das Wenden eines Blattes bzw. Nichts-Tun (zweimal Wenden ergibt wieder die Vorderseite). Nennen wir als weiteres Beispiel eine Achsenspiegelung (Klappung) an einer symmetrischen Figur (oder auch eine Punktspiegelung = Drehung um 180°), oder die Vertauschung oder Nicht-Vertauschen von zwei Elemente $\{a, b\}$, dann erhalten wir die gleiche Gruppen-Struktur wie oben.

Hintereinander Ausführung	Nichts tun	vertauschen
Nichts tun	unverändert	vertauscht
vertauschen	vertauscht	unverändert

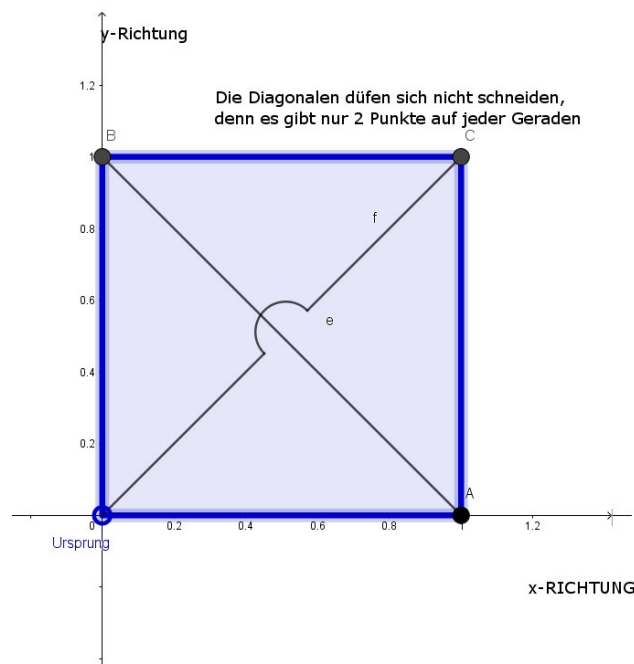
Verwendet man „**Blatt wenden**“ als Operation,
dann ergibt das zweimalige wenden so viel wie „nichts getan“
Diese Verknüpfung bildet die kleinstmögliche Gruppe.

Mit dieser minimalsten Gruppe (oder dem kleinsten denkbaren Zahlenkörper⁵) kann man nun das **Minimalst-Modell der** (Euklidischen)

⁵ Die Multiplikation als wiederholte Addition wird hier ad absurdum geführt, da es nur Null-mal und Ein-mal gibt. Die multiplikative Gruppe besteht nur aus dem Ein-mal, dem neutralen Element, da ja die Null ausgeschlossen werden muß.

Geometrie bilden, bei der jede Gerade aus genau 2 Punkten besteht und zwei Geraden sich in höchstens einem Punkt schneiden! Es gibt auch zu jeder Geraden durch jeden Punkt „außerhalb“ **genau eine Parallele**, und alle Axiome der Euklidischen Geometrie sind erfüllt.

Bei der Ebene $\{0, 1\}^2$ schneiden sich die beiden Koordinatenachsen im Ursprung $(0, 0)$ und gehen durch $(1, 0)$ bzw. die y-Achse durch $(0, 1)$. **Die ganze Ebene enthält nur noch einen weiteren Punkt, nämlich $(1, 1)$. Dadurch kann es auch nur sechs Geraden geben.**



Minimalstmodell einer euklidischen Ebene

besteht mit $(0, 0)$, $(1, 0)$, $(0, 1)$ und $(1, 1)$

aus den 4 Ecken eines Quadrats

$\{0, 1\}^2$ statt \mathbb{R}^2

Die **sechs Geraden** sind seine 4 Seiten und die beiden Diagonalen e und f, die sich allerdings nicht schneiden dürfen. Auch das **Parallelen-Axiom wird erfüllt**. Beispielsweise existiert die Parallele zur x-Achse durch den Punkt (1, 1) indem sie geht außer durch (1, 1) noch durch (0, 1) geht. Aber es gibt **keine senkrechten Geraden**⁶ und keinen rechten Winkel R von 90° , da es ja **keine Winkelgrößen** außer 0 und 1 gibt, d.h. wäre der rechte Winkel $R = 1$, dann sind zwei senkrechte Winkel wegen $1+1=0$ verschwunden und ergeben keinen gestreckten von $2R = 180^\circ$, sondern von 0° . oder 360° .

Allerdings gibt es ja auch **nur eine Länge außer der Null**. Alle Strecken (die ja eigentlich die Geraden sind) müssen also gleichlang sein; **alle**

Punkte sind also gleichweit voneinander entfernt.

Daher ist das **Koordinatensystem für dieses Modell ungeeignet**. Das Tetraeder-Modell⁷ eignet sich besser zur Darstellung dieser Ebene. **Das Modell eines Tetraeders hat auch den Vorteil, daß man sehr schön sehen kann,**

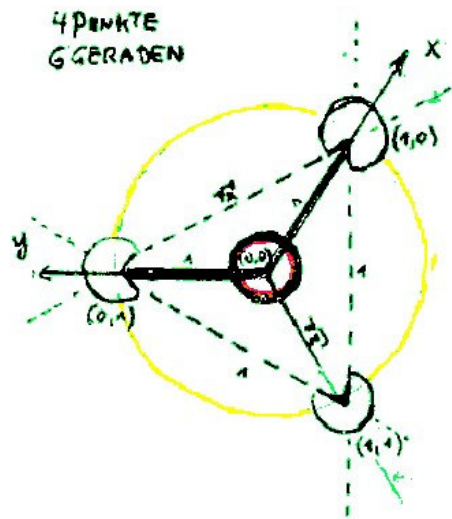
daß die Ebene $\{0, 1\}^2$ genau vier Kreise hat, nämlich jeweils um die drei Ecken des Vierflächners. Kreise können natürlich nicht aus genau zwei Punkten bestehen, da es ja sonst Geraden wären. **Kreise haben immer einen Punkt mehr als die Geraden**, also hier **genau drei Punkte**.

⁶ Das Minimalstmodell hat natürlich auch keine Mittelpunkte und keine Teilverhältnisse usw.

⁷ **Diese affine Inzidenzebene der Ordnung 2** gibt die Struktur der affinen Inzidenzebene der Ordnung 2 mit 3 Richtungen zu je 2 Geraden, vier Punkten und insgesamt 6 Geraden

Bleibt aber die Frage, ob sie auch einen Mittelpunkt haben, wenn alle Punkte voneinander immer die Entfernung 1 haben (ALTERNATIVE ist ja nur die Entfernung 0). Wenn es eine Mitte gäbe, dann käme ja nur der vierte Punkt infrage, die Pyramidenspitze, wenn die Basisfläche den Kreis enthält. Das ist aber auch eine Problematik des Pyramidenmodells (wie wohl jedes anderen $\{0, 1\}^2$ -Modells auch), daß es ist ja nicht eben, sondern räumlich! Will man das Modell mit **sich nicht schneidenden Geraden** darstellen (Stichwort FANO-Ebene), so muss man eben zur Darstellung in den Raum gehen!

Da der vierte Punkt ist ein äußerer Punkt ist, haben diese vier Kreise keinen Mittelpunkt!



Minimalstmodell $\{0,1\}^2$ der euklidischen Ebene:

Nur zwei Punkte auf jeder Geraden
und drei Geraden durch jeden Punkt

Die insgesamt sechs Geraden sind die schwarzen geraden Verbindungen

Der gelbe Kreis ist keine Gerade,

sondern wirklich ein Kreis, und eine Kreis-Spiegelung an ihm ist die Identität.

Die Kreise haben einen Punkt mehr als die Geraden!

Die Entfernung zu einem jeden andern Punkt ist ja immer 1.

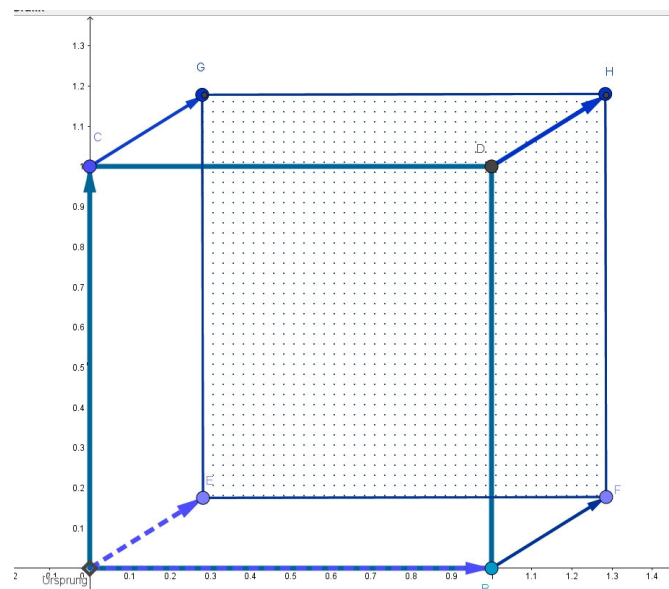
Parallelen sind Gegenkanten

Die bilden Abbildungen aller Translationen (wie üblich) eine kommutative Gruppe mit vier Elementen, bei der jedes Element zu sich selbst invers ist. Das ist die Kleinsche Vierergruppe!

Nacheinander verschieben	(0, 0)	(1, 0)	(0, 1)	(1, 1)
(0, 0)	00	(1, 0)	(0, 1)	(1, 1)
(1, 0)	10	00	(1,1)	(0, 1)
(0, 1)	01	11	00	(1; 0)
(1, 1)	11	01	10	00

Das Vertauschungsgesetz gilt für die Verschiebungsvektoren (bzw. Translationen)

Und nun betrachten wir den **kleinst-möglichen euklidischen Raum $\{0, 1\}^3$**



Minimalmodell des euklidischen Raums

$\{0, 1\}^3$ statt \mathbb{R}^3

$(0, 0, 0), (1, 0, 0), (0, 1, 0), (0, 0, 1), (1, 1, 0), (1, 0, 1)$ und $(1, 1, 1)$

besteht aus den 8 Ecken eines Würfels

und hat $(8 \text{ über } 2) = \mathbf{28}$ **Geraden** mit genau 2 Punkten

wobei jede Gerade durch genau drei Ebenen geht

14 Ebenen mit genau 4 Punkten,

wobei durch jeden Punkt genau 7 Ebenen

und genau 7 Geraden verlaufen.

Und es existieren 7 Richtungsvektoren und

7 Parallelscharen zu je 2 Ebenen

Selbstverständlich dürfen sich die Flächen- und Raumdiagonalen auch

nicht schneiden, denn sonst haben Geraden keine genau 2 Punkte mehr!

Ich habe aber davon abgesehen diese „Stecken“ einzuzichnen.

Dies war die aller kleinste als C_2

bezeichnete

>>cyclic group⁸<<

Kommen wir nun zur immer kommutativ und zyklischen

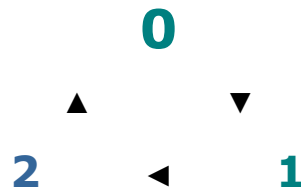
zweit-kleinsten Gruppenstruktur dritter Ordnung,

der C_3

;

⁸ Das C steht für cyclic (im Deutschen würden wir zyklisch und Z_2 schreiben!)

Die Dreiergruppe:



Die **Drei-Stunden-Uhr**

(null-eins-zwei und es geht wieder von vorne los)

0 = Teilbarkeit durch 3 Rest 0

Drehung um

0□□□□□□□□

I = Teilbarkeit durch 3 Rest 1

Drehung um 120°

Z = Teilbarkeit durch 3 Rest 2

Drehung um 240°

Diese Zahlen kann man sich (nicht auf einer Zahlengeraden, sondern auf einem Kreis als **Kreislauf (Zyklus)** vorstellen (→ Abbildung der Dreistundenuhr), oder als die endlosen Drehung um jeweils 120°, die der Addition mit Eins entspricht, wobei sich nach je drei Drehungen die Ausgangssituation immer wieder hergestellt wird.

plus	0	I	Z
0	0	I	Z
I	I	Z	0
Z	Z	0	I

Additionsgruppe mod 3

mal	I	Z
I	I	Z
Z	Z	I

Multiplikationsgruppe⁹

Beachte, dass bei der Multiplikation stets das bezüglich der Addition neutrale Element (= das Nullelement) auszuschließen ist!

⁹ Allerdings ist $I \text{ mal } I = I \text{ modulo } 3$ (da vier durch drei den Rest 1 hat) und aber auch $Z \text{ mal } Z = I \text{ modulo } 3$, aber I geteilt durch Z ist $Z \text{ modulo } 3$.

Die multiplikative Gruppe ist um das neutrale Element der Addition kleiner, denn für die Sonderzahl 0 gilt ja, dass das Produkt mit Null immer Null liefert!

$$0 \times 1 = 0 \times 2 = 0 \times 3 = \dots = 0$$

Wenn einer Faktor Null ist, verschwindet das Produkt (wird das Produkt Null!)

Wie beim Sudoku müssen aber in allen Zeilen und Spalten alle Elemente (genau einmal) vorkommen, analog der eindeutigen Auflösbarkeit von Gleichungen:

$$\text{Ist } x \circ a = y \circ a \rightarrow x = y$$

Anders ist es bei den Vierer-Restklassen, wo das Produkt zweier durch zwei teilbare Zahlen auch durch vier teilbar und somit $2 * 2 = 0$ ist.

(Nur für Restklassen modulo einer Primzahl erhält man die Körperstruktur!)

mal	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

Modulo 4

mal	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Modulo 3

Diese beiden Verknüpfungstabellen bilden keine Gruppen

Nochmals, auch auf die Gefahr hin, daß ich mich wiederhole:

Frage: Warum ist die Multiplikation mit dem Element Null keine Gruppe?

Die Null hat keinen Kehrwert (= inverses Element)

$$0 \times ? = 1,$$

es gibt also keine Zahl, die sie zur Einheit neutralisiert¹⁰

¹⁰ Wäre $0 \times \infty = 1$, dies wäre aber auch zugleich 2, denn $2 : \infty$ ist ebenfalls 0 !

Da somit die **Null kein multiplikativ-inverses** Element (keinen Kehrwert = ∞) hat, ist sie bei der Multiplikation immer auszuschließen!

Bezüglich der Addition erhalten wir bei den Restklassen immer die zyklischen Gruppen C_n . Aber bezüglich der Multiplikation hat man wegen der Nullteilerfreiheit jedenfalls für **Primzahlordnungen** die zyklische Gruppenstruktur.

Die Restklassen 1, 2 und 3 bezüglich modulo 4 (der Teilbarkeit durch 4) bilden bezüglich der Multiplikation keine Gruppe¹¹, da ja das Abgeschlossenheitsgesetz nicht gilt: **2 mal 2 ist Null** (Abbildung links).

Bezüglich der Addition erhalten wir immer die sog. zyklischen Gruppen. Aber bezüglich der Multiplikation hat man diese Gruppenstruktur nur für die Primzahlordnungen garantiert.

¹¹ Bei nicht primen Restklassen modulo n bilden diese (wie immer ohne das neutrale Element der Addition) keine multiplikative Gruppe, denn es fehlen zu den Teilern von n die inversen Elemente: Das Produkt zweier n ergebenden Teiler ergibt nämlich die Null-Restklasse; man sagt, die Null ist nicht mehr nullteilerfrei! In den Zahlkörpern ist das Produkt nämlich nur dann Null, wenn (zumindest) ein Faktor Null ist, aber z.B. für die Restklassen bezüglich der Teilbarkeit durch vier ist die Multiplikation auch Null ohne einen Faktor Null

$$\boxed{2_{\text{mod}4} \text{ mal } 2_{\text{mod}4} = 0_{\text{mod}4}} \text{ die Zwei teilt die Null.}$$

Somit wird ein Produkt zumindest für zwei Restklassenzahlen auch Null, obwohl kein

Faktor Null ist:

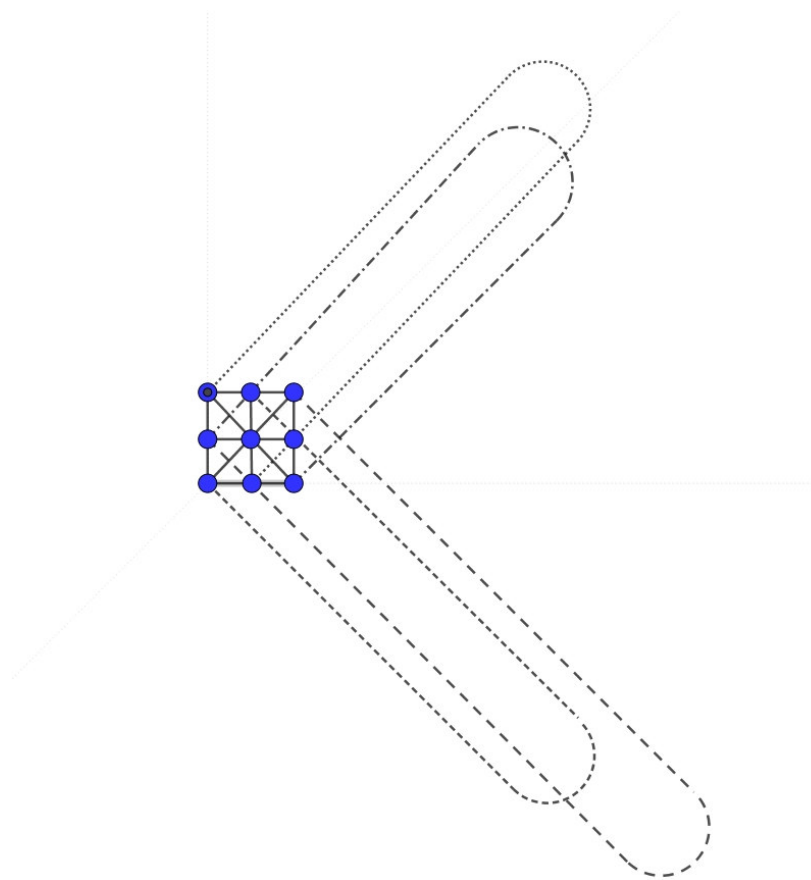
$$p \text{ mal } q = 0 \text{ mod } n \text{ (nichtprim).}$$

Mithin gibt es im Beispiel zur Zwei keinen Kehrwert, das heißt, kein Element existiert, welches, wenn mit zwei multipliziert wird, das multiplikative neutrale Element 1 ergibt.

Das zweitkleinste Minimalmodell der Euklidischen Eben $\{0, I, Z\}^2$

bzw. des Euklidischen Raums $\{0, I, Z\}^3$

Bereits bei drei Punkten auf jeder Geraden ist überhaupt keine Darstellung mit echten Geraden in der Ebene mehr möglich oder es kommt zu Schnittpunkten, die nicht sein dürfen. Hier habe ich neben den neun wirklich geraden Strecken noch eine vie weitere Geraden gestrichelt eingezeichnet, die aber nicht wirklich gerade dargestellt werden kann!

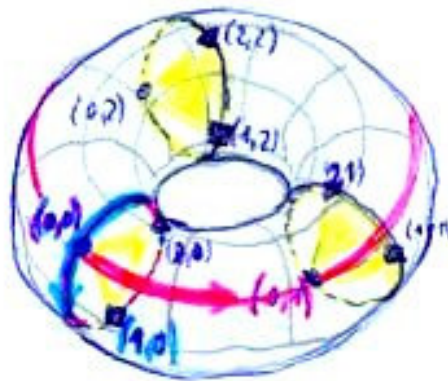


Die zweitkleinste Planimetrie mit 9 Punkten und 12 Geraden

Durch je zwei Punkte ist jede Gerade
(= Strecke) eindeutig bestimmt und aber
auf jeder Geraden liegt noch ein weiterer Punkt ,
(jede Gerade hat also genau drei Punkte)

zB. durch $(0,0,0)$, $(1,0,0)$, $(0,1,0)$ und $(1,1,0)$,
gehen durch vier Punkte!

Auf jeder Geraden liegen genau drei Punkte und durch je zwei Punkte ist eine Gerade eindeutig bestimmt, zu der es zudem eine eindeutige Parallele durch jeden der zu ihr 24 disjunkten Punkte gibt. Schon die kommutative Verknüpfungstafel der Translationen ist 27×27 groß!



$\{0, 1, 2\}^2$ als Torus-Oberfläche

Da die Achsen bei Restklassenkörpern zyklisch (also Kreise) sind, ist die wohl beste Realisation des geometrischen Modells auf einem Torus zu suchen – einem Kreis, der um einen anderen, noch größeren t drei Mal gedreht wird!

Es gibt noch andere Minimalmodelle der Geometrie, die

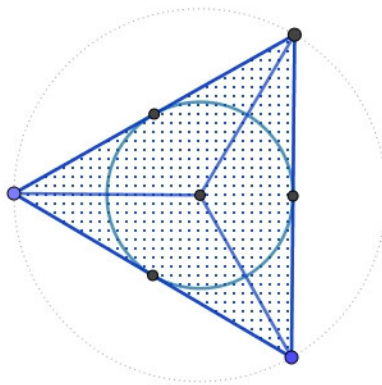
Minimalmodelle der Projektiven Ebene

Für projektive Geometrien gilt das Dualitätsprinzip:

Man kann die Begriffe Punkt und Gerade austauschen!

Dazu muss man den Begriff Verbindungsgerade mit Schnittpunkt vertauschen.

Das **Minimalst-Modell der Projektiven Ebene** besteht aus den drei Ecken eines Dreiecks mit den drei Seiten als Geraden.



Zweitkleinste projektive Minimalmodell

mit sieben Punkten und sieben Geraden,

auf denen immer genau drei Punkte liegen.

Und drei Geraden schneiden sich immer in einem Punkt. Allerdings lässt sich hier eine Gerade (die durch die drei Seitenmitten des Dreiecks) nur als Kreis darstellen!

Der äußere (kaum sichtbar gepunktete Kreis ist aber keine dazu gehörende Gerade!

Es gibt $7! = 5040$ Vertauschungen, aber nur 168 geradentreue, die zur Gruppe $PSL(2, 7)$ isomorph sind.

Definition der Ordnung projektiver Ebenen:

Die Zahl q heißt einer Ebene, wenn **jede Gerade aus genau $(q + 1)$ Punkten besteht.**

Anzahlsatz:

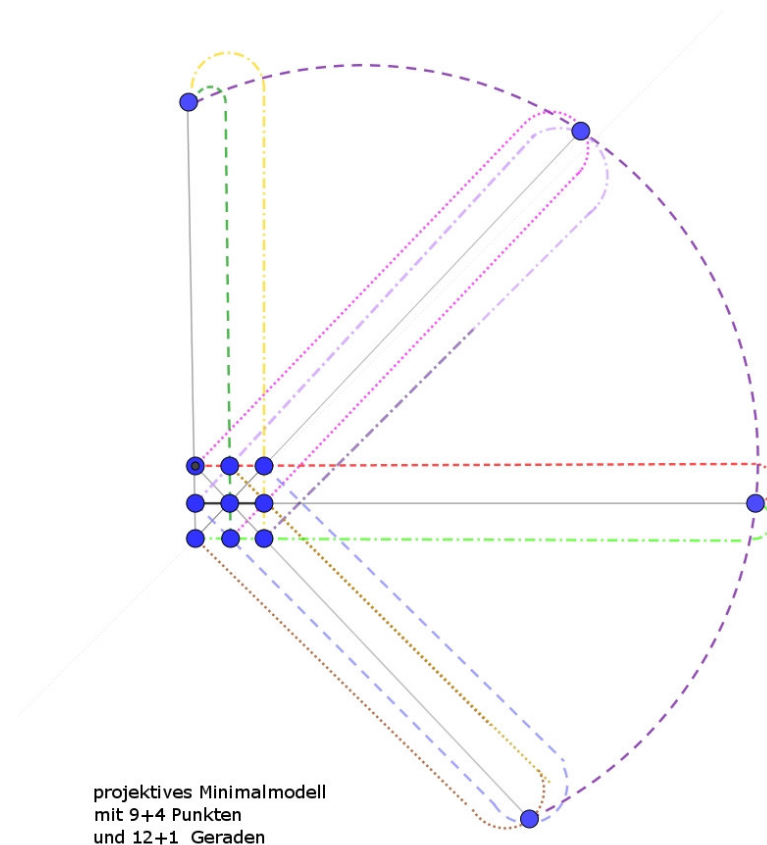
Eine projektive Inzidenzebene der Ordnung q besitzt genau $q^2 + q + 1$ Punkte und ebenso viele Geraden.

Setzt man für $q=1, 2$ oder 3 ein, dann erhält man $3, 7$ oder 13

Dazu → PDF von Prof. **Siegfried Krauter** der

Pädagogische Hochschule Ludwigsburg

>>Einführung in die Endliche Geometrie<<



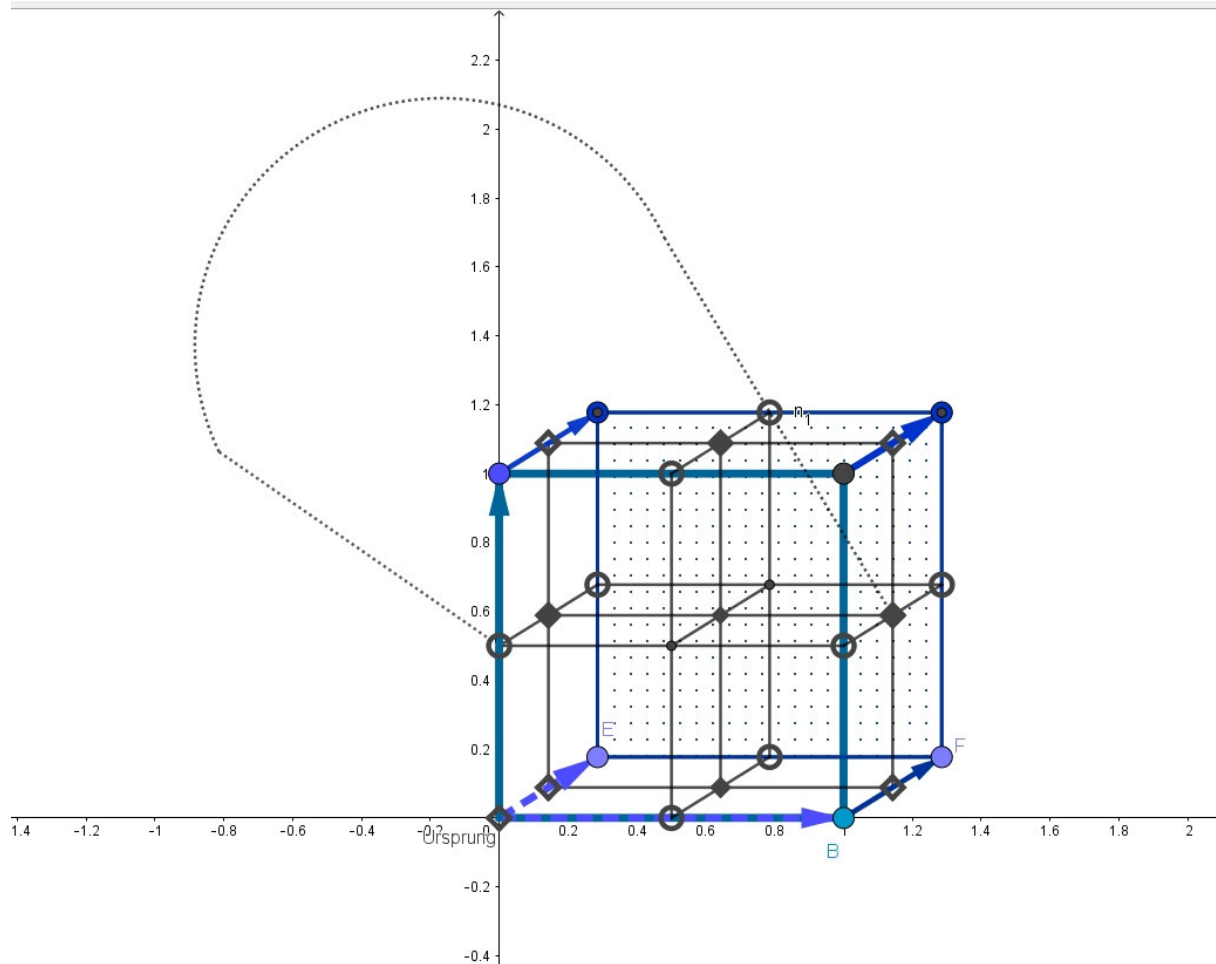
Zur Projektiven Ebene 3. Ordnung erweiterte 9-Punkte Ebene
mit 13 Punkten und 13 Geraden

Die „krummen“ Geraden sind gestrichelt und farbig
(das sind alle außer drei)

Durch die Hinzunahme der „unendlich“ fernen Punkten wird aus der neun punktigen 3 x 3-- Ebene eine **projektiven Minimal-Ebene** dritter Ordnung mit **13 Punkten und 13 Geraden** a vier Punkten (und je vier Geraden schneiden sich in genau einem Punkt). Dabei wird *jeder Parallelschar der euklidischen Ebene ein gemeinsamer „unendlich ferner“ Parallelschnittpunkt* zugeordnet und die *sämtlichen Fernpunkte liegen auf einer gemeinsamen „Ferngeraden“*. (Im Falle von unendlich vielen Geradenpunkten ist es die Gerade durch alle uneigentlichen Punkte im Unendlichen).

Umgekehrt gelangt man durch Schlitten längs einer beliebigen Gerade, also durch Herausnehmen einer Gerade und aller mit ihr inzidierenden Punkte, von einer projektiven Ebene zu einer euklidischen (affinen) Ebene.

Kommen wir nun noch zum zweitkleinsten **Minimalmodell** des Euklidischen Raumes



$\{0, 1, 2\}^3$ statt \mathbb{R}^3

Die $3^3=27$ **Punkte** des zweitkleinsten Minimalmodells des Euklidischen Raumes bilden **117 Geraden** (nur eine von denen, die nicht gerade dargestellt werden können, ist gepunktet eingezeichnet)

und 39 Ebenen zu je neun Punkten, wobei jede Gerade in zehn Ebenen liegt

und jede Ebene 12 Geraden enthält.

Durch jeden Punkt gehen 13 Ebenen (es gibt 13 Richtungsvektoren).

Es gibt nur die folgenden dreizehn verschiedenen Richtungen

$(1, 0, 0), (0, 1, 0), (0, 0, 1)$

$(1, 1, 0), (1, 0, 1), (0, 1, 1),$

$(1, 1, 1),$

$(1,2, 0) \parallel (2, 1, 0), (1, 0, 2) \parallel (2, 0, 1), (0, 1, 2) \parallel (0, 2, 1)$

$(1,1,2) \parallel (2, 2,1), (1,2, 1) \parallel (2,1,2),$ und $(2, 1, 1) \parallel (1, 2, 2)$

Durch jeden Punkt gehen daher 13 Geraden, also eine mehr, als die Anzahl der Geraden einer ganzen Ebene. Damit hat $\{0,1, 2\}^3$

$13 \times 27 : 3 =$ **117 Geraden**,

und durch jede Gerade gehen 12 Ebenen.

Es folgen nun die zwei Strukturen von vier-elementigen Gruppen

Die Gruppen 4ter Ordnung

Während die Addition immer eine zyklische Gruppe bildet, ist die **Multiplikation** (ohne das additive Nullelement) **manchmal nur eine Halbgruppe**. Bei Restklassen modulo einer Primzahl ist es aber immer auch eine zyklische Gruppe. Beide Gruppen zusammen bilden eine sog. kommutative **Körper**-Struktur, wobei noch das distributive Verteilungsgesetz gelten muss, welche die Addition und Multiplikation miteinander verknüpft.

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

Addition mod 4

*	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Multiplikation mod 5

	1	2	4	3
1	1	2	4	3
2	2	4	3	1
4	4	3	1	2
3	3	1	2	4

bzw. das **Element 3 mit 4 getauscht**

Beide Gruppen haben dieselbe zyklische Struktur.

Einen sehr schönen Beweis, der auch von **Richard E Borcherds** sehr gut erklärt ist, finden sie diese „Gruppen-Gleichheit“ in der 3. Folge seiner

‘Group theory’ über Homomorphismus:

www.youtube.com/watch?v=SUh7JBbKqVw

Ab der Ordnung vier (ab vier Elementen) gibt es nun zuweilen **verschiedene Gruppenstrukturen**, sofern es sich nicht um eine Primzahl-Ordnungen handelt, die ja immer einen zyklischen (kommutativen) Körper bilden:

Die endlichen Zahlen-Körpern (wie den Primzahlrestklassen) sind immer kommutativ, denn die Kommutativität der Multiplikation wird durch diejenige der Addition erzwungen¹².

¹² Endliche Körper sind kommutativ.

Kap.5 in Aigner-Ziegler's >>Buch der Beweise<<, Springer 2002.

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

Addition mod 4

\square	n	a	b	p
n	n	a	b	p
a	a	n	p	b
b	b	p	n	a
p	p	b	a	n

Kleinsche 4er-Gruppe

Links: Die zyklische Gruppe

(wie bei jeder additiven Gruppe ist sie aus einem einzigen Element, der EINS, erzeugbar).

Die Zeilen entstehen (insbesondere bei der Addition) durch einen **Zyklus (Kreislauf)**: Wir können uns hier die Addition auf einer **Vierstundenuhr** vorstellen. Die Zahlenrestklassen bezüglich der Teilbarkeit durch die Vier

(oder jeweils Drehungen um $0^\circ = 360^\circ$, 90° , 180° und 270° ums Zentrum) sind

- n = die Zahl ist durch vier teilbar: **Rest 0**
- a = bei der Teilung durch vier bleibt der **Rest 1**
- b = bei der Teilung durch vier bleibt der **Rest 2**
- c = bei der Teilung durch vier bleibt der **Rest 3**

Aus der ersten Zeile 0 1 2 3

wird um eins verschoben die zweite 1 2 3 0

daraus um eins verschoben die dritte 2 3 0 1

und, wenn man nochmal verschiebt, die vierte 3 0 1 2

oder was dasselbe ist:

$$0+1 = 1$$

$$1+1 = 2$$

$$2+1 = 3$$

$$3+1 = 0$$

$$0^\circ + 90^\circ = 90^\circ,$$

$$90^\circ + 90^\circ = 180^\circ,$$

$$180^\circ + 90^\circ = 270^\circ,$$

$$270^\circ + 90^\circ = 360^\circ \equiv 0^\circ \text{ (Identität)}$$

Bildet die Multiplikation keine Gruppe (sondern nur eine Halbgruppe), dann spricht man von einem (endlichen) Ring, wie z.B. der Restklassen bezüglich der Teilbarkeit durch vier (allgemein durch eine Nicht-Primzahl). Die **Matrizen** mit nicht-verschwindender Determinante bilden bezüglich der Addition und Multiplikation einen (unendlichen) Ring, wobei dieser durch die Einschränkung, dass ihre Determinante genau Eins ist, zu den flächenerhaltenden Abbildungen wird (wie die Kongruenzabbildungen der Drehungen oder Spiegelungen).

Die **zyklische Vierergruppe C_4** (die isomorph zu Addition modulo 4 ist) sind Drehungen eines Quadrats von jeweils 0, 1, 2, 3 mal 90° um sein Zentrum.

Allgemein sind diese „Strahlensymmetrien“-Gruppen des regelmäßigen n-Ecks zyklische, denn man kann die die ganze Gruppe additiv aus einem Element erzeugen. Es ergibt sich die als C_n bezeichnete zyklische Gruppe n-ter Ordnung beim regelmäßigen n-Eck durch die Drehungen um $360^\circ/n$,

Bei C_2 sind beide Elemente selbstinvers, und bei der Addition modulo 4 bilden die zwei Elemente 0 und 2 eine C_2 Untergruppe, die bekannte kleinste Gruppe der Drehungen um Null (bzw.360) Grad und 180Grad!

+	0	1
0	0	1
1	1	0

kreuz

+	n=0	e=1
n=0	n	e
e=1	e	n

+	0	1	e	n
0	0	1	e	n
1	1	0	n	e
e	e	n	0	1
n	n	e	1	0

	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

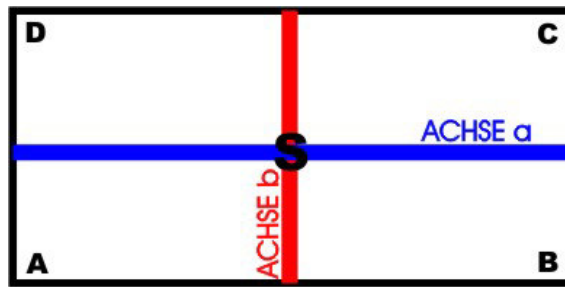
Kommen wir nun zum Produkt $C_2 \times C_2$, das aber nicht isomorph zur zyklischen Gruppe C_4 ist. (Beweis für ganz hartnäckige, die das nicht wahrhaben wollen: Group theory 5 über das Produkte von Gruppen von **Richard E Borcherds**

www.youtube.com/watch?v=H6im5UeNss)

Die zweite Vierergruppen-Struktur $C_2 \times C_2$, - die sog. **Kleinsche-, ist nicht zyklisch**, d.h. sie lässt sich nicht allein aus einem Element erzeugen. Da jedes Element zu sich selbst invers ist, ist sie aber symmetrisch: Sie enthält das neutrale Element n in der Diagonalen, bezüglich der sie gespiegelt werden kann.

Rechts ist die Kleinsche Vierergruppe mit der Diagonalen-Neutralität, und jedes Element ist zu sich selbst invers (und mit dem neutralen Element bilden sich **drei** solcher kleinsten **Untergruppen**¹³: $\{1, 2\}$, $\{1, 3\}$ und $\{1, 4\}$) . Beide sind symmetrisch bezüglich der ersten Diagonalen (also kommutativ oder abelsch). **Man denke an ein Rechteck mit a und b als Symmetrieachsenspiegelungen und p als Punktspiegelung am Schnittpunkt von a und b (=Ergebnis der zwei Klappungen).**

¹³ Wenn das neutrale Element dabei ist und das Abgeschlossenheitsgesetz gilt, erhält man eine UG.



n = nichts tun (neutral)

um 0° (bzw. 360°) um den Schnittpunkt S der beiden senkrechten Achsen drehen

a = Spiegelung an der Achse a (Klappung um die Achse a)

$A \rightarrow D$ und $B \rightarrow C$ u.u.

b = Spiegelung an der Achse b (Klappung um b)

$A \rightarrow B$ und $D \rightarrow C$ u.u.

p = die Ecken über die Diagonalen vertauschen, also **Punktspiegelung**

eine Drehung um 180° $A \rightarrow C$ und $B \rightarrow D$ u.u.

(bzw. nacheinander an den beiden senkrechten Achsen a und b spiegeln = Drehung um Schnittpunkt mit 180°)

Jedes Element der Kleinschen Vierergruppe ist - wie gesagt - zu sich selbst invers. Sie enthält die maximale Anzahl an Untergruppen (Untergruppen sind kleinere Gruppen in der Gruppe; sie müssen immer das neutrale Element enthalten!)

Zweimal hintereinander punktspiegeln ist $p \circ p = \text{Identität}$,

d. h. zweimal um 180° drehen ist also **um 360° drehen**, was als Ergebnis dasselbe ist, wie um 0° drehen oder **nichts tun**,

also **n** (neutrales Element oder identische Abbildung).

Beispielsweise ist $a \circ b = p$ (sprich „a nach b“) die Nacheinander-Ausführung zweier Klappungen (Achsen Spiegelungen) zuerst um a klappen und danach um b . Das Resultat ist

eine Drehung um den doppelten Schnittwinkel um den Schnittpunkt beider Achsen, die Punktspiegelung an Schwerpunkt, also p^{14} .

a nach p ergibt b , denn p kann ersetzt werden durch zwei Spiegelungen (allgemein an zwei beliebigen senkrecht aufeinander stehenden Achsen) das heißt also auch durch a nach b , wobei ja a zu sich selbst invers, also $a^2 = n$ ist:

$$a \circ p \circ a \circ a \circ b = a^2 \circ b \circ b$$

Das ist übrigens zugleich die Gruppe der folgenden vier 2×2 Matrizen bezüglich der Matrizen-Multiplikation:

1 0	-1 0	0 1	0 -1
0 1	0 -1	1 0	-1 0
neutrales	Punktspiegelung	die beiden Klappungen	
Element	am Ursprung (0, 0)	Spiegelung an $y=x$ und $y=-x$	

Es gibt nur diese beiden verschiedenen Vierergruppenstrukturen, die zyklische und die kleinsche. Diese zyklische Vierergruppe ist C_4 sie ist (wie gesagt) nicht das Produkt $C_2 \times C_2$

$$\{0, 1\} \times \{0, 1\} = \{0, 1\}^2,$$

In der dualen Schreibweise $1 = 01$, $2 = 10$ und $3 = 11$

kann sehr schön durch Addition diese zyklische Gruppe sehen:

+	00	01	10	11
00	00	01	10	11
01	01	10	11	00

¹⁴ Normalerweise ist es ein Unterschied, ob ich zuerst an der Geraden a und dann an b spiegele, oder ob ich zuerst um b klappe und danach erst um die Achse a : Das Ergebnis ist jeweils eine Drehung um den doppelten Schnittwinkels bezüglich des Achsenschnitts, aber in verschiedener Orientierung, also in verschiedene (positive und negative) Drehrichtungen. Die Drehung im Uhrzeigersinn (negative) um a kann durch eine Drehung mit dem Winkel $360^\circ - \alpha$ ersetzt werden.

10	10	11	00	01
11	11	00	01	10

Definiert man als Gruppen-Verknüpfung statt der Addition der binären Codes die stellenweise Addition mod 2, bei der $1+1=0$ (ist ohne Übertrag), dann erhält man die Kleinsche Gruppe $C_2 \times C_2 = C_2^2$ bei der jedes Element zu sich selbst invers ist.

	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

Die Gruppen von **Primzahlordnung** (die also p Element haben mit p ist prim) haben alle eine **eindeutige Struktur**. Es gibt daher auch nur eine einzige **Gruppenstruktur 5ter Ordnung; eine zyklische Gruppe**, nämlich die C_5

Natürlich ist die additive Gruppe der **Teilbarkeitsklassen durch 5** (Restklassen **modulo 5** genannt) eine zyklische Gruppe. Aber auch die multiplikative Gruppe mod 5, - die ja nur vier Elemente enthält, da die Null ausgeschlossen werden muss¹⁵-, ist eine „zyklische“ Vierergruppe.

mal mod5	1	2	3	4					addieren mod4	0	1	2	3
1	1	2	3	4					0	0	1	2	3
2	2	4	$6=1 \pmod{5}$	$8=3 \pmod{5}$					1	1	2	3	0
3	3	$6=1 \pmod{5}$	$9=4 \pmod{5}$	$12=2 \pmod{5}$					2	2	3	0	1
4	4	3	$12=2 \pmod{5}$	$16=1 \pmod{5}$					3	3	0	1	2

Diese beiden Gruppen sehen zunächst nicht strukturgleich (zyklisch) aus!! Sind es aber!

+ mod4	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

* mod 5	1	2	4	3
1	1	2	4	3
2	2	4	3	1
4	4	3	1	2
3	3	1	2	4

Die multiplikative Vierergruppe modulo 5 (die 0 ist nicht dabei) hat dieselbe zyklische Struktur wie die additive mod4 links, anders ist nur daß das neutrale Element nun statt 0 die 1 ist

WIE MAN SIEHT, WENN MAN DIE DREI MIT DER VIER !

¹⁵ Null hat bezüglich dem Malnehmen keinen Kehrwert:

Es gibt keine Gegennull 0^{-1} mit $0 \times 0^{-1} = 1$, so dass deren Produkt mit Null zur Einheit neutralisiert würde, denn 0^{-1} müsste Eins geteilt durch Null, also ∞ sein. Aber dies wäre zudem nicht eindeutig, da ja 0 geteilt durch jede andere Zahl ebenfalls unendlich wird!

Die **multiplikative Restklassen-Gruppe** der Teilbarkeit durch fünf (mod 5) ist somit nichts anderes als die zyklische Vierergruppe der Restklassen-Addition für die Teilbarkeit durch vier (modulo 4), was man bei Vertauschung von 3 und 4 sieht!

Das neutrale Element der Multiplikation ist wegen $a * 1 = a$ die Einheit oder das 1-Element (d.h. bei der Teilung einer Zahl bleibt der Rest 1).

Zwei Zahlen mit Rest 1 miteinander multipliziert, ergeben

$$(5n + 1)(5m + 1) = 25nm + 5(n + m) + 1$$

also wieder eine Zahl mit dem Rest 1, wenn man sie durch fünf teilt.

Entsprechend ergeben zwei Rest-Vierer-Zahlen (modulo 5) auch eine Zahl mit Rest 1 (modulo 5):

$$4_{(\text{mod } 5)} \times 4_{(\text{mod } 5)} \rightarrow (5n + 4)(5m + 4) = 5 \times 5nm + 5 \times (4n + 4m) + 16 \rightarrow 1_{(\text{mod } 5)}$$

und teilt man diese Zahl durch fünf, geht das bei den ersten beiden Summanden auf, und man muss nur noch die **16 durch fünf** teilen,

was den **Rest 1** ergibt.

Die 4 modulo 5 ist also zugleich ihre eigenes multiplikatives Gegenstück (ihr Kehrwert), denn mit sich selbst multipliziert neutralisiert sich die (Restklassen-)Vier bezüglich der Teilung durch 5.

$$16 : 5 = 3 \text{ Rest } 1 \quad \text{d.h. } \mathbf{16 = 1 \text{ mod } 5}$$

Man sagt, die Vier sei zu sich selbst invers oder zugleich ihr eigenes Inverse.

**Da 5 prim ist, bilden die Restklassen mod 5 einen kommutativen Körper.
Es gibt also nur die zyklische Struktur C_5 bei Gruppen mit 5 Elementen!**

Die Minimalebene mit vier Punkten je Gerade $\{0, 1, 2, 3\}^2$ ist auch durch einen Restklassenkörper beschreibbar, obwohl die vier keine Primzahl ist, bei der ja die Multiplikation nicht mehr nullteilerfrei! Aber das ist schon trickreich und funktioniert über sog Primkörper

Sätze über endliche Körper:

a) Die multiplikative Gruppe eines endlichen Körpers ist auch stets zyklisch.

Als Folge davon ist jeder endliche Körper kommutativ

(es gibt also keine endlichen Schiefkörper).

b) Jeder endliche Körper besitzt einen Primkörper, der zu einem Restklassenkörper isomorph ist. Daher ist die Charakteristik jedes endlichen Körpers eine Primzahl.

c) Zu jeder Primzahlpotenz p^n gibt es bis auf Isomorphie genau einen Körper.

----→ www.jmilne.org/math/CourseNotes/GT.pdf

Bei Primzahl-Anzahlen ist immer eine Körper Struktur (insbesondere eindeutige) bezüglich der Addition und Multiplikation vorhanden.

Primzahlgruppen haben ja immer nur eine (insbesondere kommutative) Struktur, nämlich die zyklische C_n . Sie sind stets die additiven Restklassen modulo n .

This ist he end, beautiful friend,
the very, very end of part I

www.youtube.com/watch?v=VScSEXrWUqQ

Eine Gruppe ist eine algebraische Struktur G mit einer assoziativen Verknüpfung $*$, in der sich Gleichungen lösen lassen, $a*x=b$ hat zu gegebenem a und b immer genau eine Lösung x . Gruppen spielen zum Beispiel als Symmetriegruppen in vielen Bereichen der Mathematik, aber auch der Physik oder Chemie eine wichtige Rolle. In der Vorlesung werden wir uns vor allem mit endlichen Gruppen beschäftigen. Geplante Themen sind: Gruppen und Untergruppen, symmetrische Gruppen, Satz von Cayley, abelsche Gruppen, zyklische Gruppen, Homomorphismen und der Homomorphiesatz, die Isomorphiesätze, Gruppenwirkungen, p -Gruppen und die Sylowsätze, endliche Körper und Matrizen­gruppen, Darstellungen.

- Stroth, Endliche Gruppen
- Aschbacher, Finite Group Theory
- Kurzweil Stellmacher, Theorie der endliche Gruppen
- Bogopolski, Introduction to Group Theory
- Jacobson, Basic Algebra I
- Cohn, Basic AlgebraX

Von mir empfohlenes **PDF** von **Prof. Siegfried Krauter**

Pädagogische Hochschule Ludwigsburg

Einführung in die
Endliche Geometrie