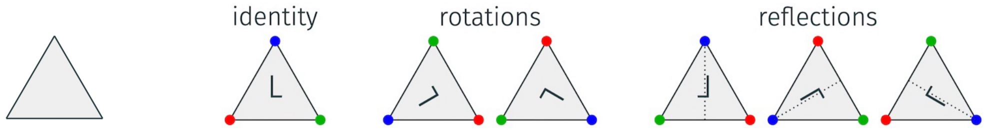
Worum geht es in den algebraischen Strukturen?

Im Prinzip um zwei fundamentale Konzepte:

Symmetrie — Allgemeinere Rechenbereiche

Symmetrie

Malen Sie mal ein (gleichseitiges) Dreieck auf ein Blatt Papier und überlegen Sie sich, was Sie damit anstellen (transformieren) können, ohne es aber eigentlich zu verändern (Symmetrie-Transformationen).



(Quelle: eigener TikZ code)

$\Rightarrow$ 6 Symmetrie-Transformationen

Interessante Erkenntnis: wendet man eine Symmetrie-Transformation an, und danach noch eine, so bekommt man eine dritte! z.B.

Drehung um 120° (Nr. 2), dann Drehung um 240° (Nr. 3) $=$ altes Dreieck (Nr. 1)

Kurzschreibweise: $3 \circ 2 = 1$ (zu lesen von rechts nach links).

Man kann also sagen: 3 macht 2 wieder rückgängig (inverse Transformation)

Weitere Erkenntnisse (zum Nachdenken):

$\rightarrow$ jede Symmetrie-Transformation hat eine inverse

$\rightarrow$ $(a \circ b) \circ c = a \circ (b \circ c)$ (Assoziativität)

$\Rightarrow$ Symmetrie-Transformationen bilden also eine Gruppe

Anderes Beispiel (ohne Geometrie): nehmen Sie ein Polynom, sagen wir $X^2 - 2$. Was sind die Nullstellen? $+\sqrt{2}$, und $-\sqrt{2}$. Das Polynom hat eine Symmetrie-Transformation, die $+\sqrt{2}$ und $-\sqrt{2}$ austauscht. Jedes Polynom hat so eine Symmetrie-Gruppe.

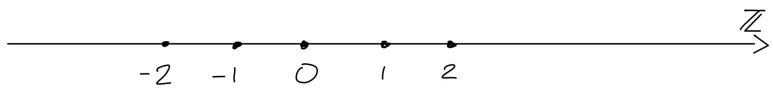
Gruppen sind eine Abstraktion der Eigenschaften von Symmetrie-Operationen eines Objekt. Das Studium von Gruppen ist ein Weg, das Konzept von Symmetrie ganz allgemein zu studieren. Wir benötigen dazu nicht unbedingt ein konkreates (reales) Objekt dessen Symmetrien wir studieren.

Warum tut man das überhaupt? Weil's schön ist!

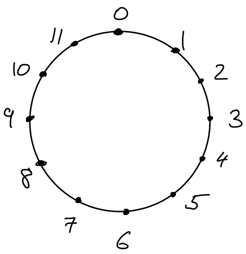
Evariste Galois
1811 – 1832
(Quelle: Wikipedia)

Allgemeinere Rechenbereiche

Sie alle kennen die ganzen Zahlen $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ und wissen wie man damit rechnet. Nehmen Sie doch anstatt der Zahlengerade



einfach mal eine Uhr



$\mathbb{Z}/12\mathbb{Z}$

Hierin können Sie auch rechnen: $5+1=6$ usw. Es passieren halt nur etwas komische Dinge: $11+1=0$, $9+5=2$ usw. Aber im Prinzip...

Anderes Beispiel: vielleicht kennen Sie die imaginäre Einheit $i=\sqrt{-1}$. Da ist garnichts imaginär dran, das ist einfach eine Nullstelle des Polynoms X^2+1, und so etwas darf man sich immer wünschen. Betrachten Sie jetzt mal Zahlen der Form

$$a + i \cdot b \ , \quad a, b \in \mathbb{Z}$$

Mit denen kann man rechnen! Z.B.

$$(2+i) + (3-7i) = 5 - 6i$$

$$(2+i)\cdot(3-7i) = 2\cdot 3 - 2\cdot 7\cdot i + 3\cdot i - 7\cdot \underbrace{i\cdot i}_{=i^2=-1} = 13 - 9i$$

Das gibt also einen erweiterten Zahlbereich $\mathbb{Z}[i]$ (<u>Gaußsche Zahlen</u>).

Gilt Primfaktorisierung in $\mathbb{Z}[i]$? Was sind überhaupt Primzahlen in $\mathbb{Z}[i]$? Schauen Sie mal:

$$2 = (1-i)(1+i)$$

$\uparrow$ Primzahl! $\nwarrow$ Faktorisierung!

Ups!?

Wir müssen mal darüber Nachdenken, was "Rechnen" und "Rechenbereich" eigentlich ist $\rightsquigarrow$ Begriff eines <u>Rings</u>.

<u>Lustige Anekdote:</u> Fermat's letzter Satz: für $n \geq 3$ hat $X^n + Y^n = Z^n$ keine positiven ganzzahligen Lösungen.
Lamé (1847): Gibt Beweis. Nimmt (ohne darüber nachzudenken) an, dass gewisse Erweiterungen von $\mathbb{Z}$ eindeutige Faktorisierung in Primzahlen haben. Stimmt aber nicht!
So richtig war das aber keinem klar, da die abstrakten Begriffe zu Rechenbereichen nicht existierten! $\rightsquigarrow$ Zusatzmaterialien: <u>BBC-Video</u>, Näheres zum Nicht-Beweis.