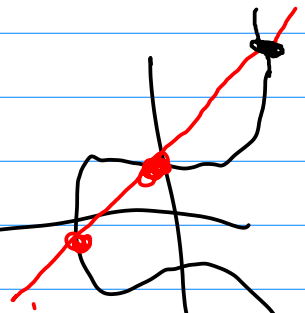
# Elliptische Kurven

$y^2 = x^3 - x - 1$

$ay^2 = bx^3 + cx^2 + dx + e$

$+ fy + gxy + hxy^2 + ix^2y$

$+ jx^3$



# Gruppen

## Gruppenstruktur

Zahl + Zahl = Zahl

Vektor + Vektor = Vektor

Punkt + Punkt = Punkt

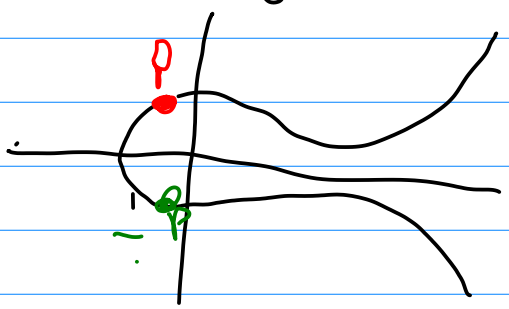
**Def.:** Wenn P, Q und R auf einer Geraden liegen, dann:

$$P + Q + R = 0$$

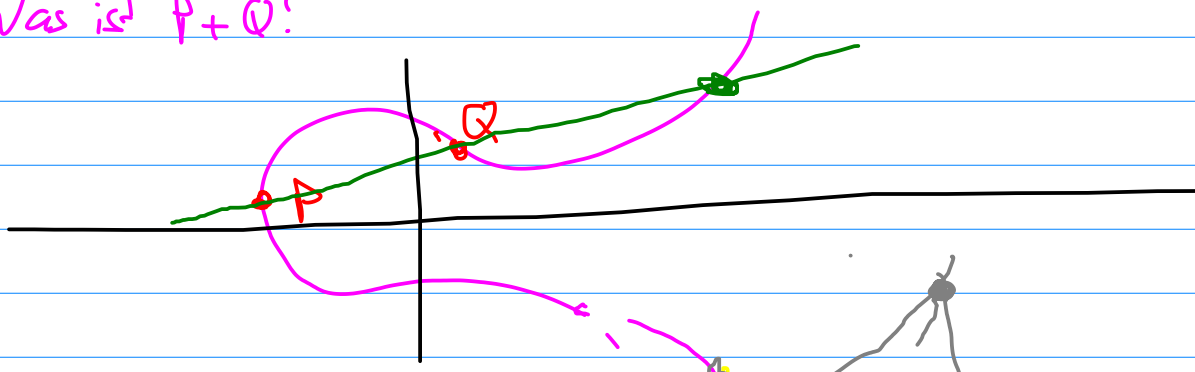
**F1:** Sei P ein Punkt auf der Kurve.
Was ist $-P$?

Probe: $P + \text{Vermutung} + O = O$

Punkt im Unendl. $=: O$

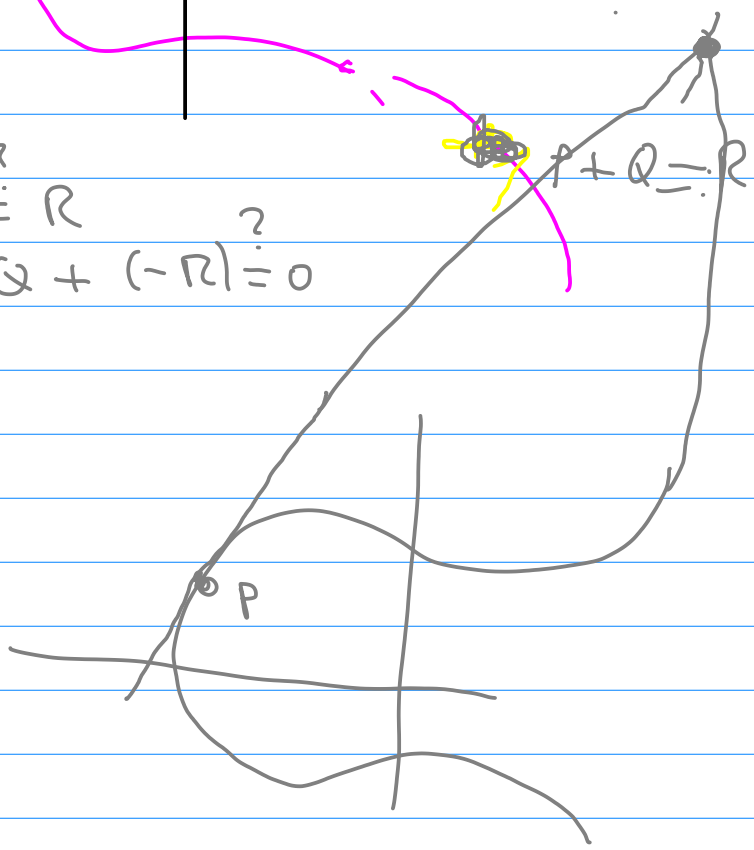


F2: Was ist $P+Q$?




$P + Q \overset{?}{=} R$

$P + Q + (-R) \overset{?}{=} 0$




Was ist $P+P$?

Wie berechnet man $10 \cdot P := \underbrace{P + P + P + \dots + P}_{10 \text{ Summanden}}$

$4P = (P+P)+(P+P) = 2\cdot(2P)$

$8P = 2\cdot(2\cdot(2\cdot P))$

$= (P+P)+(P+P)+(P+P)+(P+P)$

$12347213 \cdot P = ?$

Fakt: Gegeben $P$ und $n$, dann ist es leicht, $n \cdot P$ auszurechnen.

Aber: Gegeben $P$ und $n \cdot P$, dann ist es schwer, auf das $n$ zurückzurechnen.

Körper mit 4 Elementen:

$X^2 - 4 = (X+2)(X-2)$ reduzibel

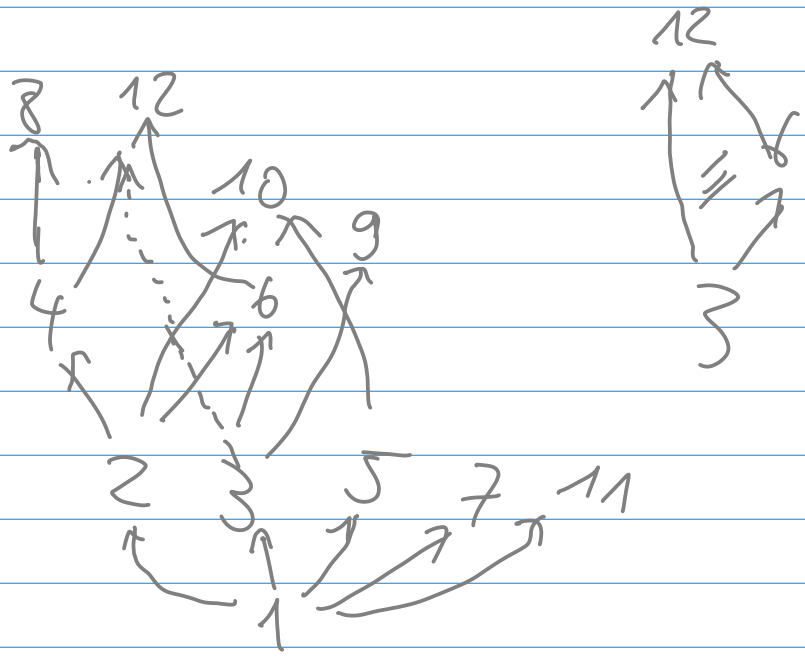
$\mathbb{Z}/(2)[X] / (X^2 + X + 1 = 0)$

$a = X$, $b = X+1$

$X^2 + 1$ irreduzibel

| + | 0 | 1 | a | b |
|---|---|---|---|---|
| 0 | 0 | 1 | a | b |
| 1 | 1 | 0 | b | a |
| a | a | b | 0 | 1 |
| b | b | a | 1 | 0 |

Körper mit 9 Elementen:
$\mathbb{Z}/(3)[X]/(X^2+X+1)$


8
12
10
9
4
6
2
3
5
7
11
1
12
6
3