Vorlesung Kryptographie

WiSe '23/'24, hhu
K. Halupczok

K19: Die Gruppenstruktur elliptischer Kurven

Stichworte:
- Definition Punktaddition $P+Q$ auf $E(k)$ mit 3. Schnittpunkt $P*Q$ von $G(P,Q) \cap E(k)$
- $\mathcal{O}$ ist neutrales Element • Invertieren leicht bei Kurzer Weierstraßform • explizite Formeln für "+"

19.1. Einleitung: Wir erhalten mit der richtigen Definition einer Punktaddition eine Gruppenstruktur elliptischer Kurven, die sie für kryptographische Zwecke interessant macht.

Vereinbarung:
Sei $E(k)$ eine elliptische Kurve über einem Körper k. (Da wir auch über Tangenten sprechen möchten, muss die Kurve nicht-singulär sein.)

19.2. Satz: (a) Seien $P, Q \in E(k)$, $P \neq Q$, $G = G(P,Q) \subseteq \mathbb{P}^2(k)$ die projektive Gerade, die P und Q verbindet.
Dann hat G noch einen dritten Schnittpunkt mit $E(k)$ gemäß Vielfachheiten gezählt (d.h. ev. P bzw. Q selbst, falls $m(P; G, E(k)) = 2$ bzw. $m(Q; G, E(k)) = 2$).

(b) Sei G die Tangente an $E(k)$ im Punkt $P \in E(k)$.
Dann hat G noch einen dritten Schnittpunkt mit $E(k)$ gemäß Vielfachheiten gezählt (d.h. ev. P selbst, falls $m(P; G, E(k)) = 3$).

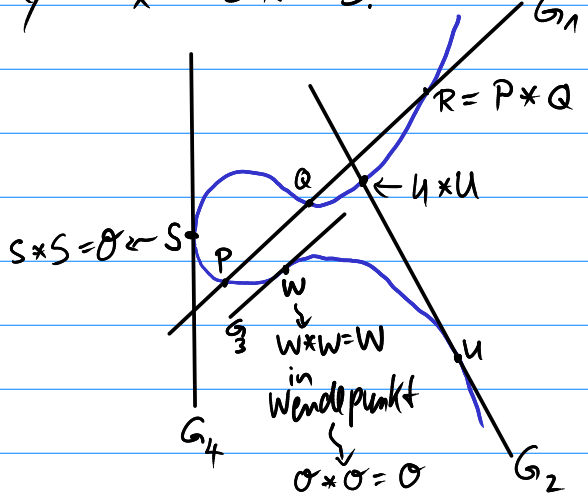
19.3. Bsp.: Der dritte Schnittpunkt kann auch der unendlich ferne Punkt $\mathcal{O} := [0:1:0]$ sein, wie etwa im Bsp. $y^2 = x^3 + 1$, mit $P = [0:1:1]$, $Q = [0:-1:1]$:
Dann ist $G(P,Q) = \{[X:Y:Z];\ X = 0\}$ ihre Verbindungsgerade, die $E(\mathbb{R})$ noch genau in $\mathcal{O} = [0:1:0]$ schneidet.

19.4. **Bew.:** Als Ergänzung zum Satz von Bézout lasen wir Satz 16.17 kennengelernt, der im Spezialfall $\deg F_1 = 1$, $\deg F_2 = 3$ dann $\sum_{P \in C_{F_1} \cap C_{F_2}} m(P, C_{F_1}, C_{F_2}) \in \{0,1,3\}$ liefert (Bsp. 16.18)).
Also gilt auch hier: $\sum_{R \in G \cap E(k)} m(R; G, E(k)) \in \{0,1,3\}$.

zu (a): Ist $G = G(P,Q)$, folgt $2 \leq \#(G \cap E(k)) \leq \sum_{R \in G \cap E(k)} m(R; G, E(k)) \in \{0,1,3\}$,
das geht nur, wenn die Vielfachensumme $= 3$ ist,
also ex. ein $R \in G \cap E(k)$
mit $R \notin \{P,Q\}$, falls $m(P; G, E(k)) = 1 = m(Q; G, E(k))$
oder mit $R = P$, falls $m(P; G, E(k)) = 2$
oder mit $R = Q$, falls $m(Q; G, E(k)) = 2$.

zu (b): Ist G die Tangente an $E(k)$ in $P \in E(k)$, ist $m(P; G, E(k)) \geq 2$ nach Satz 15.24. Es folgt wie im Beweis zu (a) wieder, dass die Vielfachensumme $= 3$ ist, also die Existenz eines $R \in G \cap E(k)$ mit $R \neq P$, falls $m(P; G, E(k)) = 2$ und $R = P$, falls $m(P; G, E(k)) = 3$ gilt. □

19.5. **Bsp.:** Betr. die elliptische Kurve $E(k)$ zur (kurzen) Weierstraßgleichung
$y^2 = x^3 - 3x + 3$. (OK, da $4 \cdot (-3)^3 + 27 \cdot 3^2 \neq 0$)



Jede Gerade, die $E(k)$ in zwei Punkten schneidet, schneidet $E(k)$ in einem dritten Punkt, gemäß Vielfachheiten gezählt. Der dritte Schnittpunkt kann auch $O \in g_\infty$ sein.

Wir möchten auf $E(k)$ eine Verknüpfung "$+$" erklären, also eine Punktaddition $P+Q$, bei der wiederum ein Punkt auf der elliptischen Kurve herauskommt. Den dritten Schnittpunkt, den die Gerade $G(P,Q)$ durch zwei Punkte P und Q auf $E(k)$ mit $E(k)$ hat (laut Satz 19.2), bezeichnen wir mit $P * Q$.

19.6. **Def.:** Für $P, Q \in E(k)$, $P \neq Q$, definieren wir also

$$P * Q := \begin{cases} R \in (G(P,Q) \cap E(k)) \setminus \{P,Q\}, \\ \quad \text{falls } m(P; G, E(k)) = 1 = m(Q; G, E(k)), \\ P, \text{ falls } m(P; G, E(k)) = 2, \\ Q, \text{ falls } m(Q; G, E(k)) = 2, \end{cases}$$

sowie

$$P * P := \begin{cases} R \in (T_P(E(k)) \cap E(k)) \setminus \{P\}, \text{ falls } m(P; T_P(E(k)), E(k)) = 2, \\ P, \text{ falls } m(P; T_P(E(k)), E(k)) = 3 \quad \text{(d.h. falls } P \text{ Wendepunkt)}. \end{cases}$$

19.7. **Bem.:** • Der unendlich ferne Punkt $O \in E(k)$ erfüllt $O * O = O$, da er ein Wendepunkt ist. • Weiter ist offensichtlich $P * Q = Q * P$ aufgrund der Def.

• Es gilt: $R = P * Q \Rightarrow P = Q * R \Rightarrow Q = R * P$, d.h. $P * (P * Q) = Q$ für alle $P, Q \in E(k)$. (*)

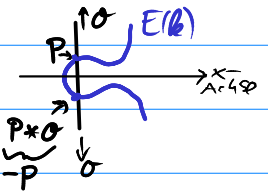
• Es gilt: $P * Q = P * R \Leftrightarrow Q = R$, denn "$\Leftarrow$", "$\Rightarrow$": Vor. $\rightsquigarrow P * (P * Q) = P * (P * R) \overset{(*)}{\Rightarrow} Q = R$.
"Kürzungsregel"

19.8. **Bem.:** Man beachte, dass für $P = [a:b:1] \in \mathbb{P}^2(k) \cap i(\mathbb{A}^2(k))$ die Gerade

$$G(P,O) = G(c,0,-a) = \{[x:y:z] \in \mathbb{P}^2(k);\ x - az = 0\}$$

im Affinen eine Parallele zur y-Achse darstellt (Gg. $x = a$).

Für eine elliptische Kurve, die durch eine Kurze Weierstraßform gegeben und (für $\mathrm{char}\, k \neq 2$) symmetrisch zur x-Achse ist, wird typischerweise $P * O \neq P$ sein.
Wegen $(O * O) * P = O * P$ einerseits, da $O * O = O$,
und $O * (O * P) = P$ andererseits, wegen ⊠,
kann die Verknüpfung $*$ also nicht assoziativ sein.
Stattdessen setzen wir unsere Verknüpfung "+" wie folgt:



19.9. **Def.:** Für $P, Q \in E(k)$ definieren wir

$$P + Q := O * (P * Q).$$

Ist $E(k)$ in Kurzer Weierstraßform und (für $\mathrm{char}\, k \neq 2$) symmetrisch zur x-Achse, erhält man $P + Q$, indem man den 3. Schnittpunkt $P * Q$ von $G(P,Q)$ mit $E(k)$ dann noch an der x-Achse spiegelt, d.h. das Negative des y-Wertes nimmt.

19.10. **Bem.:** • Es gilt: $O + P = P$, d.h. O ist neutrales Element von "+",
weil $O + P = O * (O * P) = P$ nach ⊠ gilt.
• Es gilt: $-P = O * P$, da $P + (O * P) = O * (P * (O * P))$ ⊠
$= (P * (O * P)) * O = (P * (P * O)) * O \overset{⊠}{=} O * O = O.$

Es ist nicht auf Anhieb zu sehen, dass hier mit "+" eine elliptische Kurve $E(k)$ zu einer Gruppe $(E(k), +)$ wird, speziell ob das Assoziativgesetz gilt.

19.11. **Lemma:** Liegen drei Punkte $P, Q, R \in E(k)$ einer elliptischen Kurve auf einer projektiven Geraden G, so gilt $(P + Q) + R = O$, und umgekehrt.
Dabei müssen P, Q, R nicht notwendig verschieden sein.

Bew.: Da $R = P * Q$ nach Vor., folgt $\underbrace{O * R}_{-R} = \underbrace{O * (P * Q)}_{P+Q}$, also $-R = P + Q$ bzw. $R + (P+Q) = O$.
Umgekehrt gilt das ebenso. □

19.12. **Satz (von Poincaré, 1901):** Sei k bel. Körper und $E(k)$ elliptische Kurve. Die Verknüpfung $+ : (P, Q) \mapsto P + Q$ macht $E(k)$ zu einer abelschen Gruppe $(E(k), +)$ mit neutralem Element O, d.h.
(i) $P + O = P$ für alle $P \in E(k)$,
(ii) $\forall P \in E(k)\ \exists\, Q \in E(k): P + Q = O \rightsquigarrow -P := Q$
(iii) $P + Q = Q + P$ für alle $P, Q \in E(k)$
(iv) $(P + Q) + R = P + (Q + R)$ für alle $P, Q, R \in E(k)$.

19.13. **Bem.:** Schwierig zu beweisen ist die Assoziativität in (iv). Wir behandeln diese im Vorlesungsteil K20.

19.14. **Bew. von (i)–(iii):** Zu (i): s.o. Bem. 19.10 ✓
Zu (ii): Sei $P \in E(k)$, setze $Q := O * P$, s.o. Bem. 19.10 ✓
Zu (iii): Klar aufgrund der Def von $P + Q$. ✓ □

19.15. **Bem.:**
- Anstelle O könnte man prinzipiell jeden Punkt $Q \in E(k)$ zum neutralen Element von $+$ "machen", indem man $U \boxplus V := U + V - Q$ setzt: dann ist $U \boxplus Q = U + Q - Q = U$, $U \boxplus (-U + 2Q) = U - U + 2Q - Q = Q$, und $(U \boxplus V) \boxplus W = U + V + W - 2Q = U \boxplus (V \boxplus W)$.
- Die Eigenschaft von Lemma 19.11 gilt immer noch, wenn für Q ein Wendepunkt genommen wird. Nun kann eine elliptische Kurve bis zu 9 Wendepunkten haben. [Ohne Beweis]

- Die Wahl des W.P. $\mathcal{O} := [0:1:0]$ als neutralem Element von $E(k)$ hat den Vorteil, dass die explizite Formel für "+" rechnerisch einfacher wird, weil dann die Gleichung von $E(k)$ in einfacher (langer oder kurzer) Weierstraßform vorliegt.
Diese explizite Formel wird in Satz 19.17 / Satz 19.18 angegeben.

- Invertieren, d.h. Berechnen von $-P = P * \mathcal{O}$, ist dann, bei kurzer Weierstraßform in $\mathrm{Char}\, k \neq 2$, besonders leicht:
Man spiegelt P an der x-Achse und erhält $-P$, d.h. ist $P = [a:b:c]$, gilt $-P = [a:-b:c]$. Schnittpunkte von $E(k)$ mit der x-Achse sind dann selbstinvers, d.h. $P = [a:0:c] \in E(k) \Rightarrow P = -P$.

19.16. Bsp.: Betr. $E(\mathbb{R})$ mit der Glg. $y^2 = x^3 + 17$ bzw. $y^2 z = x^3 + 17 z^3$.
Dann liegen $P = [-1:4:1]$ und $Q = [-2:3:1]$ auf der Kurve.
Ihre Verbindungsgerade ist $G(P,Q) = \{[x:y:z] \in \mathbb{P}^2(\mathbb{R});\ x - y + 5z = 0\}$.
Um $P+Q$ zu berechnen, bestimmen wir den dritten Schnittpunkt $P*Q$ von $G(P,Q)$ und $E(\mathbb{R})$ wie folgt: Setze $y = x+5$ ein und erhalte $(x+5)^2 = x^3 + 17$
$\Leftrightarrow x^3 - x^2 - 10x - 8 = 0$. Da $x=-1$, $x=-2$ Nst. der l.S. sind, führt Polynomdiv. durch $(x+1)(x+2)$ zu $x^3 - x^2 - 10x - 8 = (x+1)(x+2)(x-4)$. Der Punkt $P*Q$ hat also x-Koordinate 4, da er auf G liegt, folgt: $P*Q = [4:9:1]$, es folgt $P+Q = [4:-9:1]$.

Ist $E(k)$ gegeben durch das lange Weierstraßpolynom
$$F(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$$
bzw. $f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$, so möchten wir die Addition "+" für die Krypto-Anwendungen in einer expliziten Formel beschreiben:

19.17. **Satz:** Sei $E(k)$ gegeben durch das lange Weierstraßpolynom F. Dann gilt:

(a) $P = (u,v) \in E(k) \cap A^2(k) \Rightarrow -P = (u, -v - a_1 u - a_3)$

(b) $P = (u,v)$, $Q = (r,s) \in E(k) \cap A^2(k)$

- ist $u = r$ und $v + s + a_1 u + a_3 = 0$, gilt $P + Q = \mathcal{O}$,
- sonst ist

$$P + Q = \big(\underbrace{\lambda^2 + a_1\lambda - a_2 - u - r}_{=:x},\ -(\lambda + a_1)x - \mu - a_3\big),$$

wobei $\lambda = \dfrac{s-v}{r-u}$, $\mu = \dfrac{vr - su}{r-u}$ falls $r \neq u$,

und $\lambda = \dfrac{3u^2 + 2a_2 u + a_4 - a_1 v}{2v + a_1 u + a_3}$, $\mu = \dfrac{-u^3 + a_4 u + 2a_6 - a_3 v}{2v + a_1 u + a_3}$ falls $r = u$.

Bew.: wäre langweiliges Nachrechnen. □

Wir geben den Beweis für die Formel bei kurzer Weierstraßform, wo er leicht zu machen ist:

19.18. **Satz:** Ist $E(k)$ gg. durch $f(x,y) = y^2 - x^3 - ax - b$, so gilt:

(a) Für $P = (u,v) \in E(k)$ gilt $-P = (u, -v)$

(b) Für $P = (u,v)$, $Q = (r,s)$ mit $P \neq -Q$ ist

ist $P + Q = \big(\underbrace{\lambda^2 - u - r}_{=:x},\ \lambda(u - x) - v\big)$,

wobei $\lambda = \begin{cases} \frac{s-v}{r-u}, & \text{falls } P \neq Q, \\ \frac{3u^2 + a}{2v}, & \text{falls } P = Q. \end{cases}$

19.19. **Bem.:** Der zweite Fall in (b) mit $P = Q$ ist die "Punktverdopplung" $P + P = 2P$.

19.20. **Bew.:** (a) ✓, (b): • Sei $P \neq -Q$, $P \neq Q$.

Haben $g(P,Q) = \{(u+t, v + \underbrace{\frac{s-v}{r-u}}_{=:\lambda} t);\ t \in \mathbb{R}\}$,

sowie $f(u+t, v+\lambda t) = (v+\lambda t)^2 - (u+t)^3 - a(u+t) - b$

mit den Nullstellen $t=0$, $t=r-u$. Eine weitere Nullstelle ist $t = x-u$.

Die Nullstellensumme $0 + r-u + x-u = r+x-2u$ ergibt den Koeffizienten vor t^2 des Polynoms, nämlich $\lambda^2 - 3u$, es folgt $x = \lambda^2 - u - r$,

die y-Koordinate des Punkts auf $g(P,Q)$ ist dann $v + \lambda(x-u)$, für $P+Q$ dann das Negative.

• Ist $Q=P$, $P \neq -P$ (d.h. $v \neq 0$), nimmt man die Tangente an $E(k)$ im Punkt P,

also $t_P(E(k)) = \{(x,y);\ (-3u^2-a)x + 2vy + v^2 - 2au - 3b = 0\}$,

$= \{(u+t, v+\lambda t);\ t \in \mathbb{R}\}$ mit Steigung $\lambda := \frac{3u^2+a}{2v}$.

Der Rest der Rechnung geht wie eben, es folgt $x = \lambda^2$ (da $u=r$) und der angegebene y-Wert für $P+P$. □