Vorlesung Kryptographie

WiSe '23/'24, hhu
K. Halupczok

K20: Assoziativgesetz für elliptische Kurven

Stichworte: • Assoziativgesetz für elliptische Kurven • Neunpunktesatz als Hilfsmittel
• Bemerkungen zu anderen Beweismöglichkeiten

20.1. **Einleitung:** Wir zeigen das Assoziativgesetz für die Verknüpfung "+" auf elliptischen Kurven.

Sei $E(k)$ eine elliptische Kurve über einem Körper k. Für $P, Q \in E(k)$ hatten wir die Verknüpfung "+" definiert als $P + Q := O * (P * Q)$, dafür ist O das neutrale Element sowie $-P = O * P$ das Inverse von P. Weiter haben wir die Relation (*): $\boxed{P * (P * Q) = Q}$ für alle $P, Q \in E(k)$.

20.2. **Ziel:** Wir zeigen für eine elliptische Kurve $E(k)$ das **Assoziativgesetz**: $\forall P, Q, R \in E(k)$: $P + (Q + R) = (P + Q) + R$.

20.3. **Lemma:** Das Assoziativgesetz auf $E(k)$ gilt genau dann, wenn $\forall P, Q, R, S \in E(k)$: $(P * Q) * (R * S) = (P * R) * (Q * S)$.

Bew.: Zunächst gilt

$$P + (Q + R) = O * (P * (Q + R)), \qquad (P + Q) + R = O * ((P + Q) * R).$$

Wegen $O * (O * P) = P$ folgt:

$$O * U = O * V \iff U = V.$$

Also ist die Assoziativität äquivalent zur Gleichung

$$P * (Q + R) \stackrel{!}{=} (P + Q) * R,$$

Jetzt zur Beh. des Lemmas.

„$\Rightarrow$": wenn das Assoziativgesetz gilt, folgt mit $P * Q = -(P+Q)$

dann $\ell.g. = (P*Q)*(R*S) = -((P*Q)+(R*S))$

$= -(-(P+Q)-(R+S))$

$= (P+Q)+(R+S)$

$\overset{\text{Assoz.}}{=} (P+R)+(Q+S)$

$\overset{\text{analog}}{=} (P*R)*(Q*S) = r.g.$

„$\Leftarrow$": Gilt die Relation, folgt mit $\tilde{P}=O$, $\tilde{Q}=P*Q$, $\tilde{R}=Q*R$, $\tilde{S}=Q$

daraus $(\tilde{P}*\tilde{Q})*(\tilde{R}*\tilde{S}) = (\tilde{P}*\tilde{R})*(\tilde{Q}*\tilde{S})$,

also $(\underbrace{O*(P*Q)}_{P+Q})*(\underbrace{(Q*R)*Q}_{=R}) = (\underbrace{O*(Q*R)}_{Q+R})*(\underbrace{(P*Q)*Q}_{=P})$,

was nach obigem die Assoziativität impliziert. □

Als Beweishilfsmittel benötigen wir den

20.4. **Neunpunktesatz**: Sei k ein algebraisch abgeschlossener Körper.
Seien C_F, C_{F_1} und C_{F_2} drei kubische Kurven in $\mathbb{P}^2(k)$
zu paarweise teilerfremden homogenen Polynomen F, F_1, F_2 vom Grad 3,
und C_F enthalte 8 der 9 Schnittpunkte von $C_{F_1} \cap C_{F_2}$.
Dann liegt auch der 9. Schnittpunkt auf C_F.

20.5. Beweis (nicht vollständig, nur Beweisidee): Dass $C_{F_1} \cap C_{F_2}$ (mit Vielfachheiten gezählt) aus genau $9 = 3 \cdot 3$ Punkten besteht, besagt der Satz von Bézout, siehe Bem. 16.3.
Damit bestehen auch $C_F \cap C_{F_1}$ und $C_F \cap C_{F_2}$ aus 9 Punkten, von denen laut Vor. 8 Punkte identisch sind.

Eine allgemeine projektive kubische Kurve $\mathcal{C}$ (Singularitäten egal)
ist definiert über 10 Koeffizienten:

$$\mathcal{C}: a_1X^3 + a_2X^2Y + a_3X^2Z + a_4XY^2 + a_5XYZ + a_6XZ^2 + a_7Y^3 + a_8Y^2Z + a_9YZ^2 + a_{10}Z^3 = 0$$

- Die Kurve verändert sich nicht, wenn das kubische Polynom mit einem Skalar $s \neq 0$ multipliziert wird. Deswegen sehen wir eine kubische Kurve als einen projektiven Punkt $\underline{a} = [a_1 : a_2 : a_3 \ldots : a_{10}] \in \mathbb{P}^9(k)$ an. Betrachte nun alle kubischen Kurven, die durch die 8 vorgegebenen Punkte verlaufen. Sei $M \in k^{8 \times 10}$ die Matrix, für die die nichttrivialen Lösungen des LGS $M \cdot \underline{a} = \underline{0} \in k^8$ genau die kubischen Kurven $\underline{a} \in \mathbb{P}^9(k)$ ergeben, die durch die 8 Punkte verlaufen. Dann ist $\operatorname{rg} M \leq 8$, also folgt wegen der Dimensionsformel $\dim \ker M = 10 - \operatorname{rg} M \geq 2$.

- I.a. ist der Lösungsraum zweidimensional, d.h. $\dim \ker M = 2$, sofern die 8 Punkte in allgemeiner Lage liegen, was wir hier zur Vereinfachung annehmen möchten; liegen die Punkte in spezieller Lage, kann der Lösungsraum mind. dreidimensional werden. Zur Beweisführung sind dann umständliche Fallunterscheidungen nötig, die wir hier nicht weiter ausführen möchten.

- Ist $\dim \ker M = 2$, wird der Lösungsraum von den Koeffizienten von F_1 und F_2 aufgespannt, d.h. es ex. $r, s \in k$ mit $F = rF_1 + sF_2$. Für den 9. Schnittpunkt $[x:y:z]$ gilt $F_1(x,y,z) = 0 = F_2(x,y,z)$, und somit auch $F(x,y,y) = 0$, d.h. $[x:y:z] \in C_F$. □

20.6. Bew. der Assoziativität von "+" bei einer elliptischen Kurve $E(k)$:
O.E. sei k ein algebraisch abgeschlossener Körper (die Assoz. folgt dann für Teilkörper). Weiter genügt es, die Relation des Lemmas 20.3 nachzuweisen. Seien $P, Q, R, S \in E(k)$ und $E(k)$ durch das kubische homogene Polynom $F \in k[X,Y,Z]$ definiert.

• Wir betrachten dann die folgenden 8 Punkte:

$$P,\ Q,\ P*Q,\ R,\ S,\ R*S,\ P*R,\ Q*S, \qquad \oplus$$

diese definieren 6 Geraden G_1, G_2, G_3 und H_1, H_2, H_3 so, dass die Schnittpunkte der Geraden durch folgende Tabelle gegeben sind:

	G_1	G_2	G_3
H_1	P	Q	$P*Q$
H_2	R	S	$R*S$
H_3	$P*R$	$Q*S$	$T \in H_3 \cap G_3$

Nun ist z.z., dass der Schnittpunkt $T \in H_3 \cap G_3$ ebenfalls auf $E(k)$ liegt, denn daraus folgt dann $(P*R)*(Q*S) = T = (P*Q)*(R*S)$.

• Seien mit $G_1, G_2, G_3, H_1, H_2, H_3$ auch die linearen homogenen Polynome $\in k[X,Y,Z]$ bezeichnet, die diese Geraden definieren. Wir betrachten dann die beiden kubischen Polynome $G_1G_2G_3$ und $H_1H_2H_3$. Diese enthalten jeweils alle 9 angegebenen Punkte der Tabelle. Die elliptische Kurve trifft 8 dieser Punkte des Schnittes $C_{G_1G_2G_3} \cap C_{H_1H_2H_3}$, nämlich die Punkte der Liste $\oplus$.

• Nach dem Neunpunktesatz liegt dann auch der 9. Punkt des Schnittes, nämlich $T \in H_3 \cap G_3$, auf der elliptischen Kurve, wie z.z. war. □

20.7. Bem.: • Man kann die Assoziativität auch mithilfe der expliziten Formeln aus Satz 19.17/19.18 direkt nachrechnen, was mühsam ist.

• Algebraiker betrachten zu beliebigen algebraischen Varietäten die sogenannte Divisorklassengruppe, welche eine abelsche Gruppe laut Definition ist, sowie eine bestimmte Abb. von $E(k)$ auf ihre Divisorklassengruppe. Diese ist ein Isomorphismus nach dem tiefen Satz von Riemann-Roch, d.h. die Gruppenstruktur überträgt sich, insbesondere also die Assoziativität der Verknüpfung "+".