Satz. (Konstruierbarkeit mit Zirkel und Lineal)
Sei $\{0,1\} \subset M \subset \mathbb{C}$ und $K = \mathbb{Q}(M \cup \overline{M})$. Für ein $z \in \mathbb{C}$ sind äquivalent:

1. $z \in \mathbb{A}M$

2. Es gibt eine Kette

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_{m-1} \subset K_m = L$$

   von Teilkörpern von $\mathbb{C}$, so dass $z \in L$, $K_{i+1} = K_i(a_i)$ und $\operatorname{grad} m_{a_i,K_i} = 2$.

Beweis. 1.⇒2.: Sei $z \in \mathbb{A}M$. Nach Definition von $\mathbb{A}M$ entsteht z aus $P_0 := M$ durch eine endliche Abfolge der Schritte $P_{i+1} = P_i \cup \{w_i\}$, wobei w_i der Schnittpunkt von geeigneten

a) $\lambda, \lambda' \in Gr(P_i)$, $\lambda \neq \lambda'$,

b) $\lambda \in Gr(P_i)$, $\kappa \in Kr(P_i)$,

c) $\kappa, \kappa' \in Kr(P_i)$, $\kappa \neq \kappa'$

ist. Somit gibt es ein n mit $z \in P_n$. Setze $\tilde{K}_0 = \mathbb{Q}(M \cup \overline{M})$ und $\tilde{K}_{i+1} = \tilde{K}_i(w_i)$. Dann $P_i \subset \tilde{K}_i$ und $z \in \tilde{K}_n$.

Es bleibt zu zeigen, dass $\operatorname{grad}(m_{w_i,\tilde{K}_i}) \in \{1,2\}$. Lässt man dann alle $\tilde{K}_i$ mit $\tilde{K}_{i+1} = \tilde{K}_i$ weg, erhält man eine Kette von Teilkörpern wie im Satz gefordert.

Fall a): Eine Gerade durch $z, w \in \mathbb{C}$ ist durch die Punktemenge $\lambda = \{tz + (1-t)w \,|\, t \in \mathbb{R}\}$ gegeben. Sei genauso λ' eine Gerade durch z', w' und seien $z, z', w, w' \in \tilde{K}_i$. Ein $x \in \lambda \cap \lambda'$ erfüllt

$$tz + (1-t)w = x = sz' + (1-s)w' \ .$$

Da $\operatorname{Re}(z), \operatorname{Im}(z), \dots \in \tilde{K}_i$, erhalten wir ein lineares Gleichungssystem für t, s mit Koeffizienten in $\tilde{K}_i$. Da per Annahme $\lambda \neq \lambda'$ und $\lambda \cap \lambda' \neq \emptyset$, ist die Lösung für $r, s \in \mathbb{R}$ eindeutig und liegt in $\tilde{K}_i$ (Warum?). Somit liegt auch der Schnittpunkt $x = tz + (1-t)w$ in $\tilde{K}_i$ und es gilt $\tilde{K}_{i+1} = \tilde{K}_i$.

Fall b): Seien $z_1, z_2, p, q \in \tilde{K}_i$. Setze $r = |q|$. Schreibe

$$\lambda = \{tz_1 + z_2 \,|\, t \in \mathbb{R}\} \quad \text{und} \quad \kappa = \{w \in \mathbb{C} \,|\, |w-p|^2 = r^2\} \ .$$

Sei $w \in \lambda \cap \kappa$. Dann gilt, für ein geeignetes $t \in \mathbb{R}$,

$$w = tz_1 + z_2 \quad \text{und} \quad (w-p)(\bar{w} - \bar{p}) = r^2 \ .$$

Wir formen um:

$$\begin{aligned} & (tz_1 + z_2 - p)(t\bar{z}_1 + \bar{z}_2 - \bar{p}) = r^2 \\ \Leftrightarrow \quad & t^2 + \frac{z_1\bar{z}_2 - z_1\bar{p} + z_2\bar{z}_1 - p\bar{z}_1}{|z_1|^2} t + \frac{|z_2|^2 - z_2\bar{p} - p\bar{z}_2 + |p|^2}{|z_1|^2} - \frac{r^2}{|z_1|^2} = 0 \end{aligned}$$

Wir sehen, dass $t \in \mathbb{R}$ eine Nullstelle von $X^2 + uX + v$ ist, wobei $u, v \in \tilde{K}_i$. Dann liegt der Schnittpunkt $w = tz_1 + z_2$ in $\tilde{K}_i(t)$, und somit $\tilde{K}_{i+1} \subset \tilde{K}_i(t)$. Das Minimalpolynom $m_{t,\tilde{K}_i}$ hat Grad 1 oder 2 (da es $X^2 + pX + q$ teilt), und somit $[\tilde{K}_{i+1} : \tilde{K}_i] \leq 2$.

Fall c): So ähnlich. (Details?)

2.$\Rightarrow$1.: Wir benutzen Induktion. Nach Bem. 3 gilt $K \subset \mathcal{A}M$. Angenommen, $K_i \subset \mathcal{A}M$ für $i < m$. Da $m_{a_i,K_i} \in \mathcal{A}M[X]$ und $\mathrm{grad}(m_{a_i,K_i}) = 2$ folgt mit Satz 3, dass $a_i \in \mathcal{A}M$. Damit ist auch $K_{i+1} = K_i(a_i) \subset \mathcal{A}M$. Insgesamt ist $L = K_m \subset \mathcal{A}M$. $\square$