Exkurs: Ein galoistheoretischer Beweis des Fundamentalsatzes der Algebra

Bemerkungen:

(1) Der nachfolgende Beweis benützt zwei Eigenschaften der reellen Zahlen:
- Jedes Polynom ungeraden Grades aus $\mathbb{R}[x]$ hat (mindestens) eine reelle Nullstelle.
- Für $a \in \mathbb{R}_{\geq 0}$ existiert eine Quadratwurzel, d.h. eine Zahl $\sqrt{a} \in \mathbb{R}_{\geq 0}$ mit $(\sqrt{a})^2 = a$.

Aus der Algebra brauchen wir zwei Eigenschaften:
- Die Existenz von p-Sylowgruppen.
- Die Auflösbarkeit von p-Gruppen.

(2) Kennt man die reellen Zahlen $\mathbb{R}$, so erhält man die komplexen Zahlen durch Adjunktion von i:

$$\mathbb{C} = \mathbb{R}(i) = \{a + bi : a, b \in\} \text{ mit } i^2 = -1.$$

Der Fundamentalsatz der Algebra besagt, dass $\mathbb{R}(i)$ algebraisch abgeschlossen ist, was wir nachfolgend beweisen wollen.

Wir zeigen zunächst, dass $\mathbb{R}$ keine echten endlichen Körpererweiterungen ungeraden Grades hat:

LEMMA (A). *Ist K eine endliche Körpererweiterung von $\mathbb{R}$ von ungeradem Grad $[K : \mathbb{R}]$, so gilt schon $K = \mathbb{R}$.*

Beweis: Sei $\alpha \in K$ ein beliebiges Element. Sei $f \in \mathbb{R}[x]$ das Minimalpolynom von α über $\mathbb{R}$. Als Minimalpolynom ist f irreduzibel über $\mathbb{R}$ und erfüllt $f(\alpha) = 0$. Da $[K : \mathbb{R}]$ ungerade ist, ist wegen $[K : \mathbb{R}] = [K : \mathbb{R}(\alpha)] \cdot [\mathbb{R}(\alpha) : \mathbb{R}]$ auch $[\mathbb{R}(\alpha) : \mathbb{R}] = \operatorname{grad}(f)$ ungerade. Da f ungeraden Grad hat und normiert ist, gilt

$$\lim_{x \to -\infty} f(x) = -\infty \quad \text{und} \quad \lim_{x \to \infty} f(x) = \infty.$$

Nach dem Zwischenwertsatz für stetige Funktionen hat f (mindestens) eine reelle Nullstelle $\beta \in \mathbb{R}$. Dann lässt sich $x - \beta$ abspalten, d.h. es gibt ein Polynom $g \in \mathbb{R}[x]$ mit $f(x) = (x - \beta) \cdot g(x)$. Da f irreduzibel ist, folgt $f(x) = x - \beta$, und aus $f(\alpha) = 0$ dann $\alpha = \beta \in \mathbb{R}$. Da aber $\alpha \in K$ beliebig gewählt werden konnte, folgt $K = \mathbb{R}$, wie behauptet. ■

Das nächste Lemma zeigt, wie man aus komplexen Zahlen Wurzeln ziehen kann:

LEMMA (B). *Definiert man für $a, b \in \mathbb{R}$*

$$x = \sqrt{\frac{\sqrt{a^2 + b^2} + a}{2}} \quad \textit{und} \quad y = \operatorname{sgn}(b)\sqrt{\frac{\sqrt{a^2 + b^2} - a}{2}},$$

so gilt $x, y \in \mathbb{R}$ und

$$(x + yi)^2 = a + bi.$$

($\operatorname{sgn}(b)$ ist das Vorzeichen von b, also $b = \operatorname{sgn}(b)|b|$.)

Beweis:

- Es ist
$$\sqrt{a^2 + b^2} \pm a \geq \sqrt{a^2 + b^2} - |a| \geq \sqrt{a^2} - |a| = |a| - |a| = 0,$$
also werden durch die Ausdrücke für x und y reelle Zahlen definiert.
- Wir berechnen
$$x^2 - y^2 = \frac{\sqrt{a^2 + b^2} + a}{2} - \frac{\sqrt{a^2 + b^2} - a}{2} = a$$

und

$$\begin{aligned} 2xy &= 2\sqrt{\frac{\sqrt{a^2+b^2}+a}{2}} \cdot \operatorname{sgn}(b) \cdot \sqrt{\frac{\sqrt{a^2+b^2}-a}{2}} = \\ &= 2\operatorname{sgn}(b)\sqrt{\frac{(\sqrt{a^2+b^2}+a)(\sqrt{a^2+b^2}-a)}{4}} = \\ &= \operatorname{sgn}(b)\sqrt{(\sqrt{a^2+b^2})^2-a^2} = \operatorname{sgn}(b)\sqrt{(a^2+b^2)-a^2} = \\ &= \operatorname{sgn}(b)\sqrt{b^2} = \operatorname{sgn}(b)|b| = b. \end{aligned}$$

Wir erhalten

$$(x+yi)^2 = (x^2-y^2)+2xyi = a+bi.$$

Dies sollte gezeigt werden. ■

Bemerkung: Wie kommt man auf die Formeln für x und y im Lemma? Die Gleichung $(x+yi)^2 = a+bi$ ist gleichwertig mit dem (reellen) Gleichungssystem

$$x^2-y^2 = a, \quad 2xy = b.$$

Aus $2xy = b$ erhält man (im Allgemeinen) $y = \frac{b}{2x}$. Setzt man nun diesen Ausdruck für y in die Gleichung $x^2-y^2 = a$ ein, so kann man daraus (bis aufs Vorzeichen) x ausrechnen. Den Ausdruck für y erhält man dann aus $x^2-y^2 = a$, wobei $\operatorname{sgn}(b)$ durch die Bedingung $2xy = b$ ins Spiel kommt.

Lemma (C). *$\mathbb{R}(i)$ besitzt keine Körpererweiterung vom Grad 2.*

Beweis: Angenommen, es gäbe eine Körpererweiterung $K|\mathbb{R}(i)$ vom Grad 2. Wir wählen ein $\xi \in K \setminus \mathbb{R}(i)$. Dann gilt auch $[\mathbb{R}(i)(\xi) : \mathbb{R}(i)] = 2$. Sei $f \in \mathbb{R}(i)[x]$ das Minimalpolynom von ξ über $\mathbb{R}(i)$. Wir können schreiben

$$f(x) = x^2 + \alpha x + \beta \text{ mit } \alpha, \beta \in \mathbb{R}(i).$$

Wir machen quadratische Ergänzung:

$$f(x) = (x+\frac{\alpha}{2})^2 - \frac{\alpha^2-4\beta}{4}.$$

Mit Lemma (B) finden wir ein $\gamma \in \mathbb{R}(i)$ mit

$$\frac{\alpha^2-4\beta}{4} = \gamma^2$$

und können weiter zerlegen

$$f(x) = (x+\frac{\alpha}{2})^2 - \gamma^2 = (x+\frac{\alpha}{2}+\gamma)(x+\frac{\alpha}{2}-\gamma).$$

Dies zeigt, dass f nicht irreduzibel in $\mathbb{R}(i)[x]$ ist, ein Widerspruch. Die Annahme war also falsch, die Behauptung des Lemmas ist richtig. ■

In der Algebra zeigt man, dass jede p-Gruppe auflösbar ist. Dies ist der Inhalt des folgenden Satzes, den wir hier nochmals angeben:

Satz. *Ist G eine Gruppe der Ordnung p^n (mit einer Primzahl p und $n \in \mathbb{N}$), so existieren für $i = 0, \ldots, n$ Untergruppen G_i der Ordnung p^i, sodass G_i normal in G_{i+1} und G_{i+1}/G_i zyklisch von Ordnung p ist:*

$$G = G_n \supseteq G_{n-1} \supseteq G_{n-2} \supseteq \cdots \supseteq G_2 \supseteq G_1 \supseteq G_0 = \{e\} \quad \textit{mit} \quad |G_i| = p^i \quad \textit{und} \quad G_{i+1}/G_i \simeq \mathbb{Z}_p.$$

Wir haben nun die nötigen Hilfsmittel um den Fundamentalsatz der Algebra zu beweisen.

Satz (Fundamentalsatz der Algebra). *$\mathbb{R}(i)$ ist algebraisch abgeschlossen.*

Beweis: Sei K eine beliebige endliche Körpererweiterung von $\mathbb{R}(i)$. (Wir müssen zeigen, dass dann $K = \mathbb{R}(i)$ gilt.)

- Sei L die normale Hülle von K über $\mathbb{R}$. Dann ist $L|\mathbb{R}$ eine endliche Galoiserweiterung. Wir zerlegen
$$|\mathrm{Gal}(L|\mathbb{R})| = 2^e \cdot m \text{ mit } m \in \mathbb{N} \text{ und } 2 \nmid m.$$
(Wegen $\mathbb{R} \subseteq \mathbb{R}(i) \subseteq K \subseteq L$ ist natürlich $e \geq 1$.)
- Sei $P \subseteq \mathrm{Gal}(L|\mathbb{R})$ eine 2-Sylowgruppe von $\mathrm{Gal}(L|\mathbb{R})$. Dann ist $|P| = 2^e$. Für den Fixkörper L^P von P gilt
$$[L^P : \mathbb{R}] = \frac{[L : \mathbb{R}]}{[L : L^P]} = \frac{|\mathrm{Gal}(L|\mathbb{R})|}{|P|} = m.$$
Also ist L^P eine Erweiterung ungeraden Grades von $\mathbb{R}$. Nach Lemma (A) gilt dann $L^P = \mathbb{R}$, also $m = 1$.
- Wir haben nun also
$$|\mathrm{Gal}(L|\mathbb{R})| = 2^e.$$
- Natürlich ist auch $L|\mathbb{R}(i)$ galoissch mit
$$|\mathrm{Gal}(L|\mathbb{R}(i))| = [L : \mathbb{R}(i)] = \frac{[L : \mathbb{R}]}{[\mathbb{R}(i) : \mathbb{R}]} = 2^{e-1}.$$
- *Annahme:* Es ist $e \geq 2$. Da $\mathrm{Gal}(L|\mathbb{R}(i))$ eine Gruppe der Ordnung 2^{e-1} ist, gibt es nach dem vorangegangenen Satz aus der Gruppentheorie eine Untergruppe H der Ordnung 2^{e-2}, also $|H| = 2^{e-2}$. Für den Fixkörper L^H von H gilt $[L : L^H] = |H| = 2^{e-2}$, und damit
$$[L^H : \mathbb{R}(i)] = \frac{[L : \mathbb{R}(i)]}{[L : L^H]} = \frac{2^{e-1}}{2^{e-2}} = 2.$$
L^H wäre also eine quadratische Erweiterung von $\mathbb{R}(i)$, was aber nach Lemma (C) nicht sein kann.
- Die Annahme ist also falsch, es muss $e = 1$ gelten, und damit $[L : \mathbb{R}(i)] = 2^{e-1} = 1$, also
$$L = \mathbb{R}(i).$$
Aus $\mathbb{R} \subseteq \mathbb{R}(i) \subseteq K \subseteq L$ folgt dann
$$K = \mathbb{R}(i).$$
- Da K eine beliebige endliche Erweiterung von $\mathbb{R}(i)$ sein konnte, zeigt dies, dass $\mathbb{R}(i)$ keine echten algebraischen Erweiterungen besitzt. Dies beweist, dass $\mathbb{R}(i)$ algebraisch abgeschlossen ist. ■