Proposition 16.4 Ist $a \in L$ ($L \supseteq \mathbb{F}_p$) eine Nullstelle des Polynoms $h \in \mathbb{F}_p[X]$, so ist auch $a^p \in L$ eine Nullstelle von h.

Beweis: Es gilt $0 = h(a) = h(a)^p = (\overbrace{b_0 + b_1 a + \ldots + b_n a^n}^{h(a)})^p$ $(b_i \in \mathbb{F}_p)$

$$\overset{\text{Aufg. 98.(a)}}{=} b_0^p + b_1^p a^p + \ldots + b_n (a^p)^n$$

$$\overset{\text{Aufg. 98.(b)}}{=} b_0 + b_1 a^p + \ldots + b_n (a^p)^n = 0$$

und somit ist a^p eine Nullstelle von h. ⊣

Satz 16.5 Sei p prim und $h \in \mathbb{F}_p[X]$ ein irred. Polynom über $\mathbb{F}_p$ mit $\operatorname{grad}(h) = m \geq 2$.

(a) Ist a eine Nullstelle von h in $L \supseteq \mathbb{F}_p$, so sind $a^{p^0}, a^{p^1}, \ldots, a^{p^{m-1}}$ die m paarweise verschiedenen Nullstellen von h in L, d.h. h zerfällt in L in Linearfaktoren.

(b) Ist $a \in \mathbb{F}_{p^n}$, so gilt $m \mid n$.

Beweis: (a) Mit Prp. 16.4 sind $a^{p^0}, \ldots, a^{p^{m-1}}$ Nullstellen von h.

Wir zeigen zuerst, dass die Nullstellen paarweise versch. sind.

- Sei $1 \leq k \leq m$ die kl. Zahl mit $a = a^{p^k}$. Dann sind $a, a^p, \ldots, a^{p^{k-1}}$ paarweise versch.
- Zu zeigen: $m = k$

  In L definieren wir $g := \prod_{i=0}^{k-1} (X - a^{p^i})$.

  Dann folgt einerseits $(g)^p = (b_0 + b_1 X + \ldots + \overbrace{b_{k-1}}^{=1} X^{k-1})^p$ $(b_i \in L)$

  $$= b_0^p + b_1^p \underbrace{X^p}_{=:Y} + \ldots + \underbrace{b_{k-1}^p}_{=1} \underbrace{(X^{k-1})^p}_{=Y^{k-1}}$$

  weil $\operatorname{char}(L) = p$.

  Setzen wir $Y := X^p$, so entspricht $(g)^p$ dem Polynom $\tilde{g} \in L[Y]$ mit $\operatorname{grad}(g) = \operatorname{grad}(\tilde{g}) = k-1$.

Andererseits werden die Nullstellen von g durch das Potenzieren nur zyklisch permutiert. D.h. g und $\tilde{g}$ haben dieselben Nullstellen, und weil g und $\tilde{g}$ über L in Linearfaktoren zerfallen, gilt für alle $0 \leq i < k$, $b_i^p = b_i$ und mit Aufg. 98.(b) erhalten wir $b_i \in \mathbb{F}_p$.

Somit ist $g \in \mathbb{F}_p[X]$ und nach Konstruktion von g gilt $g \mid h$, und weil h irred. über $\mathbb{F}_p$ ist, ist $g = h$ und $k = m$.

(b) Ist $a \in \mathbb{F}_{p^n}$, so ist mit Aufg. 95.(a) sowohl a wie auch $a^p, \dots, a^{p^{m-1}}$ Nullstellen von $X^{p^n} - X$. Wir nehmen an, h sei normiert (damit ändert sich der Grad von h nicht).

Dann gilt $h \mid X^{p^n} - X$. Sei $K_h := \mathbb{F}_p(a) \cong \mathbb{F}_p[X]/(h)$.

Dann ist $|K_h| = p^m$ und es gilt, weil $K_h \subseteq \mathbb{F}_{p^n}$,

$$n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : K_h] \cdot \underbrace{[K_h : \mathbb{F}_p]}_{= m}, \quad \text{also } m \mid n.$$

Korollar 16.6 Das Polynom $X^{p^n} - X$ ist über $\mathbb{F}_p$ das Produkt aller normierten irred. Polynome vom Grad m mit $m \mid n$. Insbesondere ist die Summe der Grade dieser irred. Polynome gleich p^n.

[Beweis in den Übungen]

Proposition 16.7 Für jeden endlichen Körper K ist die Abbildung

$$\begin{array}{ccc} K & \longrightarrow & K \\ a & \longmapsto & a^p \end{array}$$

mit $p = \mathrm{char}(K)$ ein Automorphismus; die Abbildung $a \mapsto a^p$ heißt Frobeniushomomorphismus.

[Beweis in den Übungen]

17. Der algebraische Abschluss

Def. Ein Körper K ist *algebraisch abgeschlossen* wenn jedes nicht-konst. Polynom $f \in K[X]$ eine Nullstelle in K besitzt.

Bsp. $\mathbb{C}$ ist alg. abg.; endl. Körper sind nie alg. abg.; $\mathbb{Q}$ nicht alg. abg.

Lemma 17.1 Die folgenden Aussagen sind äquivalent:

(a) K ist alg. abgeschlossen.

(b) Jedes nicht-konst. Polynom $f \in K[X]$ zerfällt über K in Linearfaktoren.

(c) Jedes irred. Polynom $f \in K[X]$ hat Grad 1.

(d) Ist $L : K$ eine alg. Erweiterung, so ist $L = K$.

Beweis: (a) $\Leftrightarrow$ (b) $\Leftrightarrow$ (c) ist klar.

(c) $\Rightarrow$ (d): Sei $L : K$ alg., $a \in L$ (also a alg. über K), und sei $f \in K[X]$ das Min.-Polynom von a über K. Mit (c) gilt $\operatorname{grad}(f) = 1$, d.h. $f = (X - b)$ mit $b \in K$, und weil $f(a) = 0$ gilt $a = b$, also $a \in K$. Weil a beliebig war gilt somit $L = K$.

(d) $\Rightarrow$ (a) Sei $f \in K[X]$ mit $\operatorname{grad}(f) \geq 1$. Dann ex. mit Satz 14.6 eine einfache Erweiterung $K(a)$ von K mit $f(a) = 0$. Mit (d) ist $K(a) = K$, d.h. $a \in K$ und f besitzt eine Nullstelle in K.

⊣

Proposition 17.2 Ist $L : K$ alg. und zerfällt jedes Polynom $f \in K[X]$ über L in Linearfaktoren, so ist L alg. abg.; d.h. auch jedes Polynom $\tilde{f} \in L[X]$ zerfällt über L in Linearfaktoren.

Beweis: Sei $f \in L[X]$ irred. über L und sei a eine Nullstelle von f in einem Zerfällungskörper von f. Dann ist a alg. über L und somit auch über K ($L:K$ ist alg.). Sei $g \in K[X]$ das Min.-Poly. von a über K. Nach dem Euklidischen Alg. ex. Polynome $q, r \in L[X]$ mit $g = q \cdot f + r$ und $\text{grad}(r) < \text{grad}(f)$ oder $r = 0$. An a ausgewertet sehen wir, dass $r(a) = 0$ (weil $f(a) = 0$), woraus folgt $f \mid g$. Weil nach Voraussetzung $g \in K[X]$ über L in Linearfaktoren zerfällt, zerfällt auch das irred. Polynom $f \in L[X]$ in Linearfaktoren, d.h. $\text{grad}(f) = 1$ und L ist mit (c) alg. abg. ⊣

Def. Sei K ein Körper. Ein Erweiterungskörper L von K heißt <u>algebraischer Abschluss</u> von K, wenn $L:K$ alg. ist und jedes Polynom $f \in K[X]$ über L in Linearfaktoren zerfällt.

Bem. Ist L ein alg. von K, so enthält L alle Zerfällungskörper von Polynomen $f \in K[X]$.

Bsp. $\mathbb{C}$ ist ein alg. Abschluss von $\mathbb{R}$, aber nicht von $\mathbb{Q}$.

Satz 17.3 Jeder Körper K besitzt einen alg. Abschluss; dieser ist bis auf Isomorphie eindeutig.

Beweis-Skizze:
- Wähle eine Wohlordnung auf der Menge $K[X]$.
- Wende in jedem Schritt Satz 15.2 an; bei Limesordinalzahlen bilde Vereinigung.

⊣

Bem. Der alg. Abschluss eines Körpers ist mit Prp. 17.2 alg. abg.