9. Der Satz von Kronecker-Weber.

Ein Zahlkörper K heißt *abelsch*, wenn $K\colon \mathbb{Q}$ eine galois'sche Körpererweiterung ist und die Galois-Gruppe $\mathrm{Gal}(K\colon \mathbb{Q})$ abelsch ist. Ist die Galois-Gruppe sogar zyklisch, so können wir K einen *zyklischen* Zahlkörper nennen.

Jeder Kreisteilungskörper ist abelsch. Ist nämlich $\omega = \omega_n$ eine primitive n-te Einheitswurzel, so ist einerseits $[\mathbb{Q}[\omega]\colon \mathbb{Q}] = \phi(n)$, denn das n-te Kreisteilungspolynom ist irreduzibel und hat den Grad $\phi(n)$, andererseits liefert die Zuordnung $\omega \mapsto \omega^a$ für $1 \le a \le n$ und $(a,n) = 1$ einen Automorphismus σ_a von $\mathbb{Q}[\omega]$ (denn ω^a ist ja wieder eine primitive n-te Einheitswurzel). Wir erhalten auf diese Weise $\phi(n)$ Automorphismen von $\mathbb{Q}[\omega]$. Mehr Automorphismen kann es nach dem Dedekind-Lemma nicht geben, es ist also $\mathrm{Gal}(\mathbb{Q}[\omega]\colon \mathbb{Q}) = \{\sigma_a \mid 1 \le a \le n, (a,n) = 1\}$ und $\mathbb{Q}[\omega]\colon \mathbb{Q}$ ist galois'sch. Es ist $\sigma_a\sigma_b = \sigma_b\sigma_a$, denn $\sigma_a\sigma_b(\omega) = \omega^{ab} = \sigma_b\sigma_a(\omega)$, also ist die Galoisgruppe abelsch. All dies wissen wir natürlich schon, es wurde hier nur noch einmal zusammenfassend notiert.

Unterkörper abelscher Körper sind abelsch. Dies ist eine einfache Übungsaufgabe der Galois-Theorie: Ist K abelscher Zahlkörper und K' ein Unterkörper, so ist $K' = \mathrm{Fix}(U)$ für eine Untergruppe U von $G = \mathrm{Gal}(K : \mathbb{Q})$. Hier wird nur vorausgesetzt, dass $K\colon \mathbb{Q}$ galois'sch ist. Da U ein Normalteiler von G ist (alle Untergruppen einer abelschen Gruppe sind normal), ist $\mathrm{Fix}(U)\colon \mathbb{Q}$ wieder galois'sch und die zugehörige Galois-Gruppe ist G/U. Als Faktorgruppe einer abelschen Gruppe ist G/U abelsch.

Insgesamt sehen wir: *Jeder Unterkörper eines Kreisteilundskörpers ist ein abelscher Zahlkörper.* Es gilt auch die Umkehrung ("Kroneckers Jugendtraum"):

Satz von Kronecker-Weber. *Jeder abelsche Zahlkörper ist Unterkörper eines Kreisteilungskörpers.*

Vorbemerkung: *Sind K, L abelsche Zahlkörper, so ist auch KL abelscher Zahlkörper.* Beweis: Die Galoisgruppe von KL wird unter der Abbildung $\sigma \mapsto (\sigma|K, \sigma|L)$ in das Produkt der Galoisgruppen von K und L eingebettet. Insbesondere gilt: *Ist K abelscher Zahlkörper, so ist auch $K[\omega_n]$ abelscher Zahlkörper.*

9.1. Kronecker-Weber: Erste Reduktion.

Es genügt, abelsche Zahlkörper mit Primpotenzgrad zu betrachten.

Beweis: Jede abelsche Gruppe ist Produkt von Gruppen mit Primpotenzordnung. Wende dies auf die Galoisgruppe G des abelschen Zahlkörpers K an, sei also $G = G_1 \times \cdots \times G_m$ wobei G_m eine Gruppe mit Primpotenzordnung ist. Sei $H_i = G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_m$ und $K_i = \mathrm{Fix}(H_i)$. Dann ist K_i abelscher Zahlkörper mit Galois-Gruppe G_i, also $[K_i\colon \mathbb{Q}] = |G_i|$ hat Primpotenzordnung, und $K = K_1 \cdots K_m$. Ist nun K_i im Kreisteilungskörper $\mathbb{Q}[\alpha_i]$ enthalten (wobei α_i

eine geeignete Einheitswurzel ist), so ist K in $L = \mathbb{Q}[\alpha_1, \ldots, \alpha_m]$ enthalten, und L ist natürlich ein Kreisteilungskörper.

Es würde sogar genügen, *zyklisch Zahlkörper K mit Primpotenzordnung zu betrachten,* denn es gibt eine Zerlegung $G = G_1 \times \cdots \times G_m$, wobei alle G_i zyklische Gruppen mit Primpotenzordnung sind. Der weitere Beweis würde sich dadurch aber nicht vereinfachen.

9.2. Reduktionssatz.

Die zweite Reduktion, die wir in 9.3 durchführen wird, basiert auf dem folgenden Reduktionssatz.

Satz. *Seien $p \neq q$ Primzahlen. Sei K abelscher Zahlkörper, dessen Grad eine Potenz von p ist. Sei $q \mid \Delta_K$. Sei Q Primideal in $K[\omega_q]$ mit $q \in Q$. Sei T der Trägheitskörper von Q über $\mathbb{Q}$. Dann gilt:*

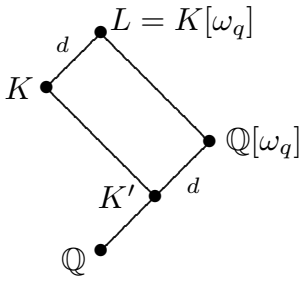
(a) $K[\omega_q] = T[\omega_q]$.

(b) $[T : \mathbb{Q}] \mid [K : \mathbb{Q}]$, *insbesondere ist der Grad von T wieder eine p-Potenz.*

(c) *Die Primteiler von Δ_T sind die von q verschiedenen Primteiler von Δ_K.*

Beweis: Sei $L = K[\omega_q] = K \cdot \mathbb{Q}[\omega_q]$.

(1) Wir zeigen als erstes: $[L\colon K] = d \cdot [K\colon \mathbb{Q}]$ *mit* $d \mid p-1$. Da K und $\mathbb{Q}[\omega_q]$ abelsche Zahlkörper sind, ist auch das Kompositum L ein abelscher Zahlkörper. Der Unterkörper $K' = K \cap \mathbb{Q}[\omega_q]$ von $\mathbb{Q}[\omega_q]$ habe Index d in $\mathbb{Q}[\omega_q]$, dann ist d ein Teiler von $q-1$ und $[L : K] = [\mathbb{Q}[\omega_q]\colon K'] = d$.

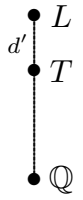


(2) *Die Primteiler der Diskriminante von L sind genau die Primteiler von Δ_K.* Beweis: Die Primteiler von Δ_L sind die Primzahlen, die Δ_K oder $\Delta_{\mathbb{Q}[\omega_q]}$ teilen. Nun ist $\Delta_{\mathbb{Q}[\omega_q]}$ eine Potenz von q und nach Voraussetzung gilt $q \mid \Delta_K$.

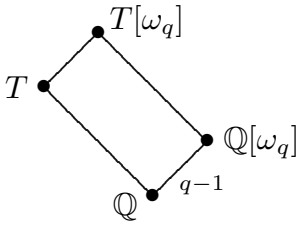
Sei nun Q Primideal in $\mathcal{O}_L$ mit $q \in Q$ und sei $\mathcal{T}$ die zugehörige Trägheitsgruppe und $T = \mathrm{Fix}(\mathcal{T})$ der Trägheitskörper.

(3) *Es ist $[L\colon T] = |\mathcal{T}|$ ein Teiler von $q-1$.* Beweis: Sei $\mathcal{V}_1$ die erste Verzweigungsgruppe zum Primideal Q. Nach 7.4 (b) ist $\mathcal{V}_1$ eine q-Gruppe, aber q ist kein

Teiler von $[L\colon \mathbb{Q}]$, siehe (1). Demnach ist $\mathcal{V}_1 = \{1\}$. Nach 7.5 (c) ist die Ordnung d' von $\mathcal{T} = \mathcal{T}/\mathcal{V}_1$ ein Teiler von $q-1$.



(4) $[T[\omega_q]\colon T] = q-1$. Beweis. Die Primzahl q ist in T nicht verzweigt, aber in $\mathbb{Q}[\omega_q]$ total verzweigt. Also ist $T' = T \cap \mathbb{Q}[\omega_q] = \mathbb{Q}$ und $[T[\omega_q]\colon T] = [\mathbb{Q}[\omega_q]\colon \mathbb{Q}] = q-1$.



(a) *Es ist* $L = T[\omega_q]$. Dazu schaue man sich nur die Inklusionskette

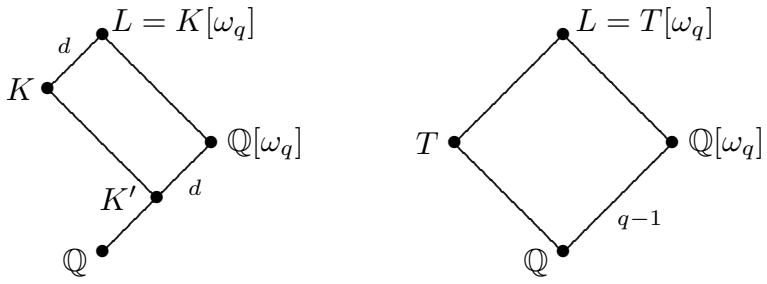
$$T \subseteq T[\omega_q] \subseteq L$$

an und verwende (1) und (4).

(b) Aus (4) und (5) folgt $[L\colon T] = q-1$, zusammen mit (1) liefert dies $[T\colon \mathbb{Q}] \mid [K\colon \mathbb{Q}]$.

(c) In (2) haben wir gesehen, dass die Primteiler von Δ_L genau die Primteiler von Δ_K sind; die Primteiler von Δ_T sind die von q verschiedenen Primteiler von Δ_L. Damit ist der Satz bewiesen.

Insgesamt sollte man sich noch einmal den Übergang von K zu T vor Augen verführen:



Da K' ein Unterkörper von K ist, ist $[K'\colon \mathbb{Q}]$ ein Teiler von $[K\colon \mathbb{Q}]$. Sei etwa $[K\colon \mathbb{Q}] = p^t$ und $[K'\colon \mathbb{Q}] = p^s$ mit $0 \le s \le t$. Es ist $q-1 = [\mathbb{Q}[\omega_q]\colon \mathbb{Q}] = d \cdot p^s$, also ist $[T\colon \mathbb{Q}] = p^{t-s}$, dies präzisiert die Behauptung (b).

Um einen Kreisteilungskörper zu finden, in dem K enthalten ist, können wir wegen (a) statt K den Körper L betrachten. Wie (b) zeigt, ist auch $[T\colon \mathbb{Q}]$ eine p-Potenz,

und die Anzahl der verzweigten Primzahlen hat sich um 1 verringert. Im nächsten Abschnitt wird dieses Induktionsargument noch einmal explizit vorgeführt.

9.3. Kronecker-Weber: Zweite Reduktion.

Es genügt, abelsche Zahlkörper zu betrachten, bei denen Grad und Diskriminantenbetrag Potenzen der gleichen Primzahl sind.

Sei K abelscher Zahlkörper vom Grad p^t für eine Primzahl p. Die von p verschiedenen Primteiler der Diskriminante Δ_K seien $q_1, \ldots, q_r$ (paarweise verschieden).

Wende den Satz 9.2 auf $K = K_0$ an. Wir erhalten einen Unterkörper $K_1 = T \subseteq K[\omega_{q_1}]$, dessen Grad ebenfalls eine Potenz von p ist, so dass die von p verschiedenen Primteiler des Diskriminantenbetrags die Zahlen $q_1, \ldots, q_{r-1}$ sind und für den

$$K[\omega_{q_1}] = K_1[\omega_{q_1}]$$

gilt. Nach r Schritten erhalten wir demnach einen Körper K_r, dessen Grad eine Potenz von p ist, dessen Diskriminantenbetrag höchstens den Primteiler p hat und für den gilt:

$$K[\omega_{q_1}, \ldots, \omega_{q_r}] = K_r[\omega_{q_1}, \ldots, \omega_{q_r}]$$

(dabei kann $K_r = \mathbb{Q}$ sein). Es bleibt also zu zeigen, dass K_r in einem Kreisteilungskörper enthalten ist.

Wir müssen jetzt also nur noch abelsche Zahlkörper betrachten, deren Grad und Diskriminantenbetrag beide Potenzen derselben Primzahl p sind. Dabei werden wir unterscheiden, ob p ungerade oder gerade ist. Zuerst wird der Fall einer ungeraden Primzahl p diskutiert.

9.4. Der Unterkörper von $\mathbb{Q}[\omega_{p^2}]$ vom Grad p, für eine Primzahl $p > 2$.

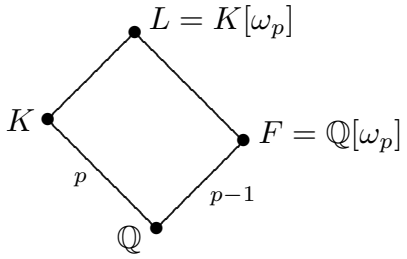
Sei $p > 2$ Primzahl.

Satz. *Es gibt nur eine Galois-Erweiterung $K\colon \mathbb{Q}$ vom Grad p, sodass $|\Delta_K|$ eine p-Potenz ist, nämlich den Unterkörper von $\mathbb{Q}[\omega_{p^2}]$ vom Grad p.*

Beweis: Es ist $[\mathbb{Q}[\omega_{p^2}]\colon \mathbb{Q}] = p(p-1)$ und $\mathbb{Q}[\omega_{p^2}]\colon \mathbb{Q}$ ist galois'sch mit Galois-Gruppe $C_{p(p-1)} = C_p \times C_{p-1}$. Diese Gruppe besitzt eine Untergruppe der Ordnung $p-1$, also besitzt $\mathbb{Q}[\omega_{p^2}]$ einen Unterkörper K vom Grad p. Da K Unterkörper von $\mathbb{Q}[\omega_{p^2}]$ ist, ist p die einzige Primzahl, die Δ_K teilt. Beachte: Da $C_{p(p-1)}$ nur eine Untergruppe der Ordnung $p-1$ besitzt, gibt es in $\mathbb{Q}[\omega_{p^2}]$ nur einen Unterkörper vom Grad p; der Körper K ist also auf diese Weise eindeutig bestimmt.

Sei nun umgekehrt K ein normaler Zahlkörper vom Grad p, und sei $|\Delta_K|$ eine p-Potenz. Setze $\omega = \omega_p$ und $F = \mathbb{Q}[\omega]$. Für $1 \leq a < p$ sei $\sigma_a \in \mathrm{Gal}(F\colon \mathbb{Q})$ durch $\sigma_a(\omega) = \omega^a$ definiert.

Wir bilden das Kompositum $L = K \cdot \mathbb{Q}[\omega]$ von K und F. Da $[K\colon \mathbb{Q}] = p$ und $[F : \mathbb{Q}] = p - 1$, ist $[L\colon \mathbb{Q}] = p(p-1)$.



Unser Ziel ist es, $L = \mathbb{Q}[\omega_{p^2}]$ zu zeigen. Dazu analysieren wir, wie L aus F entsteht.

[Hier ist der Beweis nachzutragen]

9.5. Der Unterkörper von $\mathbb{Q}[\omega_{p^{t+1}}]$ vom Grad p^t, für eine Primzahl $p > 2$.

Satz. *Sei $p > 2$ Primzahl und $t \in \mathbb{N}_1$. Es gibt genau einen abelschen Zahlkörper $K = K_{p^t}$ mit $[K\colon \mathbb{Q}] = p^t$, dessen Diskriminantenbetrag eine p-Potenz ist, nämlich den Unterkörper K von $\mathbb{Q}[\omega_{p^{t+1}}]$ mit $[K\colon \mathbb{Q}] = p^t$.* Diese Körper bilden einen Körperturm

$$K_p \subset K_{p^2} \subset K_{p^3} \subset \cdots .$$

Beweis: Sei $G = \mathrm{Gal}(\mathbb{Q}[\omega_{p^{t+1}}]\colon \mathbb{Q})$. Es ist

$$G = U(\mathbb{Z}/p^{t+1}) = C_{p^t} \times C_{p-1},$$

dabei bezeichnen wir mit C_r die zyklische Gruppe der Ordnung r. Der Körper $K = \mathrm{Fix}(C_{p-1})$ hat den Grad p^t über $\mathbb{C}$. Es gibt also einen Unterkörper $\mathbb{Q}[\omega_{p^{t+1}}]$ mit $[K\colon \mathbb{Q}] = p^t$. Die Diskriminante Δ_K ist ein Teiler der Diskriminante des Kreisteilungskörpers $\mathbb{Q}[\omega_{p^{t+1}}]$, also eine Potenz von p.

Seien nun K, K' abelsche Zahlkörper mit Grad und Diskriminantenbetrag beides Potenzen von p. Sei $L = KK'$ das Kompositum, auch dies ist ein abelscher Zahlkörper mit Grad und Diskriminantenbetrag beides Potenzen von p. Die Galois-Gruppe $G = \mathrm{Gal}(L\colon \mathbb{C})$ ist eine p-Gruppe, die eine einzige maximale Untergruppe besitzt: Ist U eine maximale Untergruppe von G, so hat G/U die Ordnung p, also ist $\mathrm{Fix}(U)$ ein abelscher Zahlkörper vom Grad p, dessen Diskriminantenbetrag eine Potenz von p ist. Nach 9.4 folgt $\mathrm{Fix}(U) = \mathbb{Q}[\omega_{p^2}]$, ein eindeutig bestimmer Körper. Eine abelsche p-Gruppe mit einer einigen maximalen Untergruppe ist aber zyklisch, und ihre Untergruppen bilden eine Kette. Die Galois-Entsprechung zeigt, dass die Unterkörper von K eine Kette bilden, also gilt $K \subseteq K'$ oder $K' \subseteq K$. Haben also K, K' den gleichen Grad über $\mathbb{Q}$, so folgt $K = K'$.