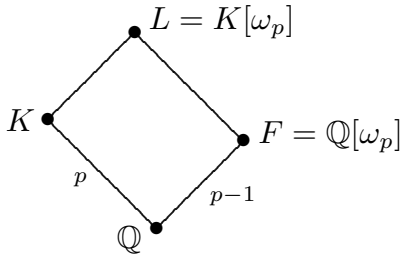
9.4. Der Unterkörper von $\mathbb{Q}[\omega_{p^2}]$ vom Grad p, für eine Primzahl $p > 2$.

Satz. *Sei $p > 2$ Primzahl. 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 $1 \le a < p$ 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.

(1) (Kummer-Theorie) *Es gibt $\alpha \in L \setminus F$ mit $\alpha^p \in F$*, demnach ist

$$L = F[\alpha] = F[\sqrt[p]{\mu}] \text{ mit } \mu = \alpha^p \in F.$$

Beweis: Sei $\eta \in \mathrm{Gal}(K\colon \mathbb{Q})$ ein Element der Ordnung p. Die Linearkombination $\sum_{i=0}^{p-1} \omega^i \eta^i$ ist nicht die Null-Abbildung (Dedekind-Lemma), also gibt es $\beta \in L$ mit

$$\alpha\colon = \sum_{i=0}^{p-1} \omega^i \eta^i(\beta) \neq 0.$$

Wende η an:

$$\begin{aligned}\eta(\alpha) &= \sum_{i=0}^{p-1} \omega^i \eta^{i+1}(\beta) \\ &= \omega^{-1} \sum_{i=0}^{p-1} \omega^{i+1} \eta^{i+1}(\beta) \\ &= \omega^{-1} \sum_{i=0}^{p-1} \omega^i \eta^i(\beta) = \omega^{-1}\alpha.\end{aligned}$$

denn $\omega^p\eta^p(\beta) = \beta = \omega^0\eta^0(\beta)$. Es folgt, dass α nicht zu F gehört (denn $\alpha \in F$ impliziert $\eta(\alpha) = \alpha$, aber wegen $\alpha \neq 0$ ist $\alpha \neq \omega^{-1}\alpha$). Außerdem sehen wir:

$$\eta(\alpha^p) = (\eta(\alpha))^p = (\omega^{-1}\alpha)^p = \alpha^p,$$

also ist $\alpha^p \in F$.

Wir wissen also:

$$L = F[\sqrt[p]{\mu}] \text{ für ein } \mu \in F.$$

Die weiteren Überlegungen dienen dazu, derartige Elemente μ zu untersuchen, und sie abzuändern, bis wir schließlich sehen, dass wir für μ eine Einheitswurzel nehmen können. Da $L\colon \mathbb{Q}$ galois'sch ist, ist die Einschränkungsabbildung

$$\mathrm{Gal}(L\colon \mathbb{Q}) \to \mathrm{Gal}(F\colon \mathbb{Q})$$

surjektiv, der Automorphismus σ_a von F lässt sich also zu einem Automorphismus von L fortsetzen, den wir ebenfalls mit σ_a bezeichnen.

(2) (Noch einmal Kummer-Theorie). *Sei* $0 \neq \alpha \in L$ *und* $\mu = \alpha^p \in F$. *Ist* $L\colon \mathbb{Q}$ *abelsch, so ist* $\dfrac{\sigma_a(\mu)}{\mu^a} \in (F^*)^p$, *für alle* $1 \leq a \leq p-1$.

Beweis: Sei $\eta \in \mathrm{Gal}(L\colon F)$ ein erzeugendes Element. Da η ein Automorphismus von L ist, gilt:

$$\frac{\eta(\alpha^a)}{\alpha^a} = \Big(\frac{\eta(\alpha)}{\alpha}\Big)^a.$$

Nun ist aber $\frac{\eta(\alpha)}{\alpha}$ eine p-te Einheitswurzel, denn α ist eine Nullstelle des Polynoms $X^p - \mu \in F[X]$ und alle Nullstellen dieses Polynoms haben die Form $\omega^i\mu$ mit $0 \leq i \leq p-1$, also sind die zu μ konjugierten Elemente von der Form $\omega^i\mu$; das Element $\eta \in \mathrm{Gal}(L\colon F)$ bildet μ auf eines dieser Elemente ab.

Es ist $\frac{\eta(\alpha)}{\alpha} = \omega^i$ für ein i, also $(\omega^i)^a = \sigma_a(\omega^i)$. Also sehen wir:

$$\Big(\frac{\eta(\alpha)}{\alpha}\Big)^a = \sigma_a\Big(\frac{\eta(\alpha)}{\alpha}\Big) = \frac{\sigma_a\eta(\alpha)}{\sigma_a\alpha} = \frac{\eta\,\sigma_a(\alpha)}{\sigma_a\alpha},$$

denn σ_a ist ein Automorphismus und nach Voraussetzung gilt $\sigma_a\eta = \eta\sigma_a$.

Insgesamt sehen wir: $\dfrac{\eta(\alpha^a)}{\alpha^a} = \dfrac{\eta\,\sigma_a(\alpha)}{\sigma_a\alpha}$, also auch $\dfrac{\eta\,\sigma_a(\alpha)}{\eta(\alpha^a)} = \dfrac{\sigma_a(\alpha)}{\alpha^a}$. Wegen

$$\eta\Big(\frac{\sigma_a(\alpha)}{\alpha^a}\Big) = \frac{\eta\,\sigma_a(\alpha)}{\eta(\alpha^a)} = \frac{\sigma_a(\alpha)}{\alpha^a},$$

ist $\dfrac{\sigma_a(\alpha)}{\alpha^a} \in F$ (und natürlich von Null verschieden, also in F^*). Demnach ist

$$\frac{\sigma_a(\mu)}{\mu^a} = \frac{\sigma_a(\alpha^p)}{\alpha^{pa}} = \Big(\frac{\sigma_a(\alpha)}{\alpha^a}\Big)^p \in (F^*)^p.$$

Bemerkungen. Erstens, es gilt auch die Umkehrung: Gibt es zu jedem a ein $\xi \in F^*$ mit $\sigma_a(\mu) = \xi^p \mu^a$, so ist $L\colon \mathbb{Q}$ abelsch.

Zweitens: In Hilbert's Theorie der algebraischen Zahlen ist dies Satz 147, mit der Formulierung: "Man beweist leicht die Tatsachen". In neueren Darstellungen (etwa Washington, Lemma 14.7) wird die Argumentationsweise formalisiert: man schreibt

$$\langle \eta, \mu \rangle = \frac{\eta(\alpha)}{\alpha} \qquad \text{falls} \qquad \alpha \in F^* \text{ und } \alpha^p = \mu$$

und nennt dies die "Kummer-Paarung" (mit Werten in $\{1, \omega, \ldots, \omega^{p-1}\}$). Hier handelt es sich um den Beginn der Entwicklung einer Kohomologie-Theorie!

(3) *Wir können annehmen:* $\mu \notin \langle 1-\omega \rangle$.

Beweis. Sei r maximal mit $(1-\omega)^r \mid \mu$. Wir zeigen, dass r eine p-Potenz ist (deswegen kann μ durch $\mu(1-\omega)^{-r} \in \mathcal{O}_K$ ersetzt werden). Wegen (2) gibt es $\xi \in F^*$ mit

$$\sigma_2(\mu) = \xi^p \mu^2.$$

Es ist $\langle \mu \rangle = \langle 1-\omega \rangle^r \cdot I$ mit $I \not\subseteq \langle 1-\omega \rangle$. Sei $\langle \xi \rangle = \langle 1-\omega \rangle^s \cdot J$, mit $s \in \mathbb{Z}$ und einem Produkt J von Primidealen $P \neq \langle 1-\omega \rangle$ mit ganzzahligen Exponenten.

Wende σ_2 auf diese Ideale an. Es ist $\langle 1-\omega \rangle$ das einzige Primideal in $\mathcal{O}_F$, das p enthält, es wird also unter jedem Automorphismus von F auf sich abgebildet (und alle anderen Primideale werden untereinander vertauscht).

Insgesamt sehen wir

$$\langle 1-\omega \rangle^r \cdot \sigma_2(I) = \langle \sigma_2(\mu) \rangle = \langle \xi \rangle^p \langle \mu \rangle^2 = \langle 1-\omega \rangle^{sp} \cdot J^p \cdot \langle 1-\omega \rangle^{2r} \cdot I^2$$

Die eindeutige Primidealzerlegung liefert: $sp + r = 0$, also ist r ein Vielfaches von p.

Die Behauptung (3) besagt, dass wir annehmen können, dass μ nicht im maximalen Ideal $\langle 1-\omega \rangle$ von $\mathcal{O}_F$ enthalten ist. Es sei daran erinnert, dass dies das einzige Primideal von $\mathbb{Z}[\omega]$ ist, das über dem Primideal $\mathbb{Z}p$ von $\mathbb{Z}$ liegt, und $\langle 1-\omega \rangle$ ist die einzige Verzweigung, die es überhaupt gibt.

Nun betrachten wir die anderen maximalen Ideale von $\mathbb{Z}[\omega]$.

(4) *Wir können annehmen, dass μ auch in keinem anderen maximalen Ideal von $\mathbb{Z}[\omega]$ enthalten ist.*

Für diesen Beweisschritt müssen wir leider auf die Originalarbeit von Lemmermeyer verweisen: *Kronecker-Weber via Stickelberger.* Journal de Theorie des Nombres de Bordeaux 17 (2005), 555-558.

An dieser Stelle geht entscheidend ein, dass in L nur die Primzahl p verzweigt ist. Man zeigt, dass das von μ erzeugte Hauptideal die p-te Potenz eines Ideals I ist.

Um zu zeigen, dass I ein Hauptideal ist, wird die Klassengruppe von F betrachtet (was denn sonst?). Stickelberger hat gezeigt, wie man von geeigneten Idealen zeigen kann, dass sie Haupideale sind. Im Fall des Ideals I lässt sich dies anwenden: I ist ein Hauptideal, etwa $I = \langle\alpha\rangle$ mit $\alpha \in F$.

Man zeigt auf diese Weise $\mu = \alpha^p\eta$, wobei η ein invertierbares Element in $\mathcal{O}_F$ ist. Natürlich ist dann

$$L = F[\sqrt[p]{\mu}] = L = F[\sqrt[p]{\alpha^p\eta}] = F[\sqrt[p]{\eta}].$$

Wir sehen also:

(4′) *L entsteht aus F durch Adjunktion der p-ten Wurzel eines invertierbaren Elements η von F.*

(5) $L = F[\sqrt[p]{\omega}]$.

Beweis. Man kann η als Produkt einer p-ten Einheitswurzel ω^r (mit $0 \le r < p$) und einer reelle Einheit ϵ schreiben (8.6), also $\eta = \omega^r\epsilon$.

Betrachte den Automorphismus σ_{-1} von F, dies ist gerade die komplexe Konjugation (denn $\omega^{-1} = \overline{\omega}$). Also ist $\sigma_{-1}(\epsilon) = \epsilon$. Daher gilt:

$$\sigma_{-1}(\eta) = \sigma_{-1}(\omega^r\epsilon) = \omega^{-r}\epsilon.$$

Wegen (2) gibt es $\xi \in F^*$ mit

$$\sigma_{-1}(\eta) = \xi^p\eta^{-1} = \xi^p\omega^{-r}\epsilon^{-1}.$$

Aus $\omega^{-r}\epsilon = \xi^p\omega^{-r}\epsilon^{-1}$ folgt $\epsilon^2 = \xi^p$.

Ist $\alpha = \sqrt[p]{\eta}$, so ist $\alpha^2 \notin F$, denn sonst wäre $p = [L\colon F] \le 2$. Demnach ist $L = F[\alpha^2]$. Aber

$$(\alpha^2)^p = \eta^2 = (\omega^r\epsilon)^2 = \omega^{-2r}\xi^p,$$

und demnach

$$L = F[\alpha^2] = F[\sqrt[p]{\omega^{-2r}}] = F[\sqrt[p]{\omega}].$$

9.6. Der Fall $p = 2$. Hier gilt ein entsprechender Eindeutigkeitssatz:

Satz. *Es gibt genau einen reellen abelschen Zahlkörper $K = K_{2^t}$ mit $[K\colon\mathbb{Q}] = 2^t$, dessen Diskriminantenbetrag eine 2-Potenz ist, nämlich den eindeutig bestimmten Unterkörper $K \subset \mathbb{Q}[\omega_{2^{t+2}}]$ mit $[K\colon\mathbb{Q}] = 2^t$. Diese Körper bilden einen Körperturm*

$$K_2 \subset K_{2^2} \subset K_{2^3} \subset \cdots.$$

Die Klassifikation der quadratischen Zahlkörper zeigt:

Lemma. *Es gibt nur drei Zahlkörper $K\colon\mathbb{Q}$ vom Grad 2, sodass $|\Delta_K|$ eine 2-Potenz ist, nämlich die Körper $\mathbb{Q}[\sqrt{2}], \mathbb{Q}[\sqrt{-1}], \mathbb{Q}[\sqrt{-2}]$.*

Daraus folgt, dass es nur einen rellen Zahlkörper $K\colon\mathbb{Q}$ vom Grad 2 gibt, sodass $|\Delta_K|$ eine 2-Potenz ist, nämlich $K = \mathbb{Q}[\sqrt{2}]$. Dies ist der entscheidende Spezialfall von Satz 9.6. Um den Satz 9.6 auf diesen Spezialfall zurückzuführen, argumentiert man wie in 9.5: Man zeigt, dass man mit einer Galois-Gruppe arbeitet, die eine einige Untergruppe vom Index 2 besitzt, also zyklisch ist.