8.2. Der allgemeine Fall.

Satz. *Sei $n \in \mathbb{N}_1$, sei ω_n eine primitive n-te Einheitswurzel und $K = \mathbb{Q}[\omega_n]$. Dann gilt:*
(a) $[K : \mathbb{Q}] = \phi(n)$,
(b) Φ_n *ist irreduzibel,*
(c) $\mathcal{O}_K = \mathbb{Z}[\omega_n]$.
(d) *Eine Primzahl teilt genau dann Δ_K, wenn sie n teilt.*
(e) *Eine Primzahl ist genau dann in K verzweigt, wenn sie n teilt.*

Beweis: Schreibe $n = p_1^{e_1} \cdots p_r^{e_r}$ mit paarweise verschiedenen Primzahlen p_i und Exponenten $e_i \geq 1$, für $1 \leq i \leq r$. Wir wollen die Aussagen (a), (c), (d) mit Induktion nach r beweisen. Den Fall $r = 1$ haben wir in 8.1 betrachtet. Sei nun $r \geq 2$. Sei $n' = p_1^{e_1} \cdots p_{r-1}^{e_{r-1}}$. Sei α eine primitive n'-te Einheitswurzel und β eine primitive $p_r^{e_r}$-te Einheitswurzel. Dann ist $\alpha\beta$ eine primitive n-te Einheitswurzel. Es ist also $K = \mathbb{Q}[\omega_n]$ das Kompositum von $\mathbb{Q}[\alpha]$ und $\mathbb{Q}[\beta]$. Nach Induktion gelten die Aussagen (a), (c), (d) für $\mathbb{Q}[\alpha]$ und natürlich auch für $\mathbb{Q}[\beta]$. Da die einzigen Primzahlen, die $\Delta_{\mathbb{Q}[\alpha]}$ teilen, die Primzahlen $p_1, \ldots, p_{r-1}$ sind, und der Betrag der Diskriminante $\Delta_{\mathbb{Q}[\beta]}$ eine Potenz von p_r ist, sind die beiden Diskriminanten teilerfremd. Wir können also Satz 6.8 an wenden. Wir sehen als erstes:

$$[K : \mathbb{Q}] = [\mathbb{Q}[\alpha] : \mathbb{Q}] \cdot [\mathbb{Q}[\beta] : \mathbb{Q}] = \phi(n')\phi(p_r^{e_r}) = \phi(n),$$

also die Behauptung (a). Nach Induktion hat $\mathbb{Q}[\alpha]$ eine Ganzheitsbasis, die nur Potenzen von α enthält, entsprechend hat $\mathbb{Q}[\beta]$ eine Ganzheitsbasis, die nur Potenzen von β enthält. Nach 6.8 besitzt also $\mathcal{O}_K$ eine Ganzheitsbasis, die nur Elemente der Form $\alpha^a\beta^b$ mit ganzzahligen Exponenten enthält. Mit α und β ist auch $\alpha^a\beta^b$ eine Potenz von ω_n, wir sehen also:

$$\mathcal{O}_K \subseteq \mathbb{Z}[\omega_n] \subseteq \mathcal{O}_K,$$

damit ist (c) gezeigt. Auch (d) folgt natürlich unmittelbar aus 6.8. Da ω_n eine Nullstelle von Φ_n ist und Φ_n den Grad $\phi(n)$ hat, folgt (b) aus (a). Nach 6.6 sind die Aussagen (d) und (e) äquivalent.

8.3. Die Galois-Gruppe $\mathrm{Gal}(\mathbb{Q}[\omega_n] : \mathbb{Q})$.

Satz. *Sei $1 \leq a \leq n$ und $(a, n) = 1$. Dann wird durch $\omega \mapsto \omega^a$ ein Automorphismus σ_a von $\mathbb{Q}[\omega_n]$ definiert* (und natürlich ist $\sigma_a(\omega^i) = (\omega^i)^a$ für alle i). *Die Zuordnung $a \mapsto \sigma_a$ ist ein Gruppen-Isomorphismus*

$$U(\mathbb{Z}/n) \longrightarrow \mathrm{Gal}(\mathbb{Q}[\omega_n] : \mathbb{Q})$$

und die Körpererweiterung $\mathbb{Q}[\omega_n] : \mathbb{Q}$ ist galois'sch.

Beweis. Seien $1 \leq a, b \leq n$ und $(a, n) = 1 = (b, n)$. Es ist

$$\sigma_a\sigma_b(\omega) = \sigma_a(\omega^b) = \sigma_a(\omega)^b = (\omega^a)^b = \omega^{ab} = \sigma_{ab}(\omega).$$

Dies zeigt, dass die genannte Abbildung ein Gruppen-Homomorphismus ist. Die Abbildung ist injektiv, denn ist $\sigma_a = \sigma_b$, so ist $\omega^a = \sigma_a(\omega) = \sigma_b(\omega) = \omega^b$, und damit $a = b$. Nun ist $|U(\mathbb{Z}/n)| = \phi(n)$ also erhalten wir die folgende Ungleichungskette

$$\phi(n) = |U(\mathbb{Z}/n)| \leq |\operatorname{Gal}(\mathbb{Q}[\omega_n]\colon \mathbb{Q})| \leq [\mathbb{Q}[\omega_n]\colon \mathbb{Q}] \leq \phi(n),$$

dabei liefert die Injektivität der Zuordnung $\overline{a} \mapsto \sigma_a$ das erste Kleiner-Gleich-Zeichen, das Dedekind-Lemma das zweite Kleiner-Gleich-Zeichen, und die Tatsache, dass ω_n eine Nullstelle des Kreisteilungspolynoms Φ_n ist, das dritte Kleiner-Gleich-Zeichen (wir setzen also nicht voraus, dass wir wissen, dass Φ_n irreduzibel ist: unsere Vergleichskette liefert einen neuen Beweis dafür!).

Alle drei Kleiner-Gleich-Zeichen können also durch Gleichheitszeichen ersetzt werden. Das zweite Gleichheitszeichen besagt, dass die Körpererweiterung $\mathbb{Q}[\omega_n]\colon \mathbb{Q}$ galois'sch ist, das erste zeigt, dass die Zuordnung $\overline{a} \mapsto \sigma_a$ bijektiv ist: Es gilt also:

$$\boxed{U(\mathbb{Z}/n) = \operatorname{Gal}(\mathbb{Q}[\omega_n]\colon \mathbb{Q})}$$

(das Gleichheitszeichen ist die kanonische Isomorphie $\overline{a} \mapsto \sigma_a$, jeder Restklasse $\overline{a}$ wird der Körper-Automorphismus von $\mathbb{Q}[\omega_n]$ zugeordnet, der jede Einheitswurzel auf ihre a-te Potenz abbildet). Das dritte Gleichheitszeichen liefert erneut einen Beweis, dass Φ_n irreduzibel ist.

Folgerungen. *Die Galois-Gruppe* $\operatorname{Gal}(\mathbb{Q}[\omega_n]\colon \mathbb{Q})$ *ist abelsch.*

Beweis: Die Gruppe $U(\mathbb{Z}/n)$ ist abelsch.

Die Struktur der Gruppe $U(\mathbb{Z}/n)$ ist bekannt (siehe Merkzettel), damit also auch die Struktur von $\operatorname{Gal}(\mathbb{Q}[\omega_n]\colon \mathbb{Q})$. Dies soll hier explizit formuliert werden, dabei bezeichnen wir mit $C_n = (\mathbb{Z}/+)$ die zyklische Gruppe der Ordnung n.

(a) *Sei* $n = p_1^{e_1} \cdots p_r^{e_r}$ *mit paarweise verschiedenen Primzahlen. Dann ist*

$$\boxed{\operatorname{Gal}(\mathbb{Q}[\omega_n]\colon \mathbb{Q}) = \operatorname{Gal}(\mathbb{Q}[\omega_{p_1^{e_1}}]\colon \mathbb{Q}) \times \cdots \times \operatorname{Gal}(\mathbb{Q}[\omega_{p_5^{e_r}}]\colon \mathbb{Q})}$$

(b) *Ist* p *ungerade Primzahl, und* $n = p^t$ *mit* $t \geq 1$, *so ist die Galois-Gruppe* $\operatorname{Gal}(\mathbb{Q}[\omega_n]\colon \mathbb{Q})$ *zyklisch,* und zwar ist

$$\boxed{\operatorname{Gal}(\mathbb{Q}[\omega_n]\colon \mathbb{Q}) = C_{(p-1)p^{t-1}} = C_{p-1} \times C_{p^{t-1}}}$$

(b) *Ist* $p = 2$, *und* $n = p^t$, *so ist* $\operatorname{Gal}(\mathbb{Q}[\omega_2]\colon \mathbb{Q}) = C_1$, *und für* $t \geq 2$

$$\boxed{\operatorname{Gal}(\mathbb{Q}[\omega_{2^t}]\colon \mathbb{Q}) = C_2 \times C_{2^{t-2}}.}$$

8.4. Primzahlen in der arithmetischen Progression $1, 1+n, 1+2n, \ldots$.

(Wir verwenden hier eigentlich nur die Definition der Kreisteilungspolynome.)

Satz. *Zu jeder natürlichen Zahl n gibt es unendlich viele Primzahlen p mit $p \equiv 1 \mod n$.*

Beweis: Wir zeigen folgendes Lemma.

Lemma. *Sei n eine natürliche Zahl und p eine Primzahl, die n nicht teilt. Genau dann gibt es ein $a \in \mathbb{Z}$ mit $p \mid \Phi_n(a)$, wenn $p \equiv 1 \mod n$ gilt.*

Beweis: Sei $a \in \mathbb{Z}$ mit $p \mid \Phi_n(a)$. Wegen $\Phi_n(a) \mid a^n - 1$ ist die Ordnung d der Restklasse von a in $\mathbb{Z}/p$ ein Teiler von n. Wir zeigen $d = n$. Wäre d ein echter Teiler von n, so wäre p Teiler von $a^d - 1$, also wäre

$$p^2 \mid (a^d - 1)\Phi(a) \mid a^n - 1.$$

Aus $a^d - 1 \equiv 0 \mod p$ folgt, dass auch $(a+p)^d - 1 \equiv 0 \mod p$ gilt. Aus $\Phi_n(a) \equiv 0 \mod p$ folgt, dass auch $\Phi_n(a+p) \equiv 0 \mod p$ gilt. Also

$$p^2 \mid ((a+p)^d - 1)\Phi(a+p) \mid ((a+p)^n - 1) = (a^n + na^{n-1}p + \ldots) - 1.$$

Modulo p^2 sehen wir:

$$0 \equiv (a^n + na^{n-1}p + \ldots) - 1 \equiv na^{n-1}p \mod p^2,$$

aber p ist kein Teiler von n und auch kein Teiler von a. Damit haben wir $d = n$ gezeigt. Nun hat die Gruppe $(\mathbb{Z}/p)^*$ die Ordnung $p-1$, also ist die Ordnung eines jeden Elements dieser Gruppe ein Teiler von $p-1$, also $n \mid p-1$. Damit ist eine Richtung gezeigt (nur diese wird weiter unten gebraucht).

Umgekehrt sei $n \mid p-1$. Die Gruppe $(\mathbb{Z}/p)^*$ ist eine zyklische Gruppe der Ordnung $p-1$, hat also ein Element $\overline{a}$ der Ordnung n. Also

$$p \mid a^n - 1 = \prod_{d|n} \Phi_d(a).$$

Ist d ein echter Teiler von n, so würde aus $p \mid \Phi_d(a) \mid a^d - 1$ folgen, dass die Ordnung von a ein Teiler von d wäre, Widerspruch. Also gilt: $p \mid \Phi_n(a)$.

Beweis des Satzes. Angenommen, es gibt nur endlich viele Primzahlen p mit $n \mid p-1$, etwa $p_1, \ldots, p_t$. Betrachte die Zahlen $\Phi_n(zp_1 \cdots p_t)$ mit $z \in \mathbb{N}$. Das Polynom Φ_n hat den Grad $\phi(n) \geq 1$ und ist normiert, also ist $\Phi_n(zp_1 \cdots p_n) > 1$ für $z \gg 0$. Sei p eine Primzahl mit $p \mid \Phi_n(zp_1 \cdots p_t)$ für ein z. Das Lemma zeigt, dass n ein Teiler von $p-1$ ist, also $p = p_i$ für ein i. Also

$$p_i \mid \Phi_n(zp_1 \cdots p_t) \mid (zp_1 \cdots p_t)^n - 1,$$

Widerspruch.

Bemerkungen. (1) Für $n = 1$, also $\Phi_1 = X - 1$ entspricht dies dem üblichen Beweis für die Existenz unendlich vieler Primzahlen.

(2) Es handelt sich um einen Spezialfall des Dirichlet-Satzes über Primzahlen in arithmetischen Progressionen (hier betrachtet man die arithmetische Progression $1, 1+n, 1+2n, 1+3n, \ldots$.) Hier die Formulierung des allgemeinen Satzes: *Ist* $(a, m) = 1$, *so gibt es unendlich viele Primzahlen* p *mit* $p \equiv a \mod n$.

(3) Warum ist gerade dieser Spezialfall von Interesse? Beachte: Für $t \geq 1$ ist $\phi(p^t) = (p-1)p^{t-1}$, und natürlich ist $(p-1, p^t) = 1$. Es ist also $p-1$ der größte zu p teilerfremde Teiler von $\phi(p^t)$. Die hier bewiesene Behauptung besagt gerade: *Es gibt unendlich viele Primzahlen* p, *sodass* n *ein Teiler von* $p-1$ *ist.* Dies bedeutet:

Folgerung. *Sei* $n \geq 1$ *eine natürliche Zahl. Dann gibt es unendlich viele Primzahlen* p, *sodass der Kreisteilungskörper* $\mathbb{Q}[\omega_p]$ *(hier ist* ω_p *eine primitive* p*-te Einheitswurzel) einen Unterkörper* K *vom Grad* p *besitzt.*

Beweis: Ist n ein Teiler von $p-1$, etwa $p-1 = nn'$, so besitzt $\mathrm{Gal}(\mathbb{Q}[\omega_p]\colon \mathbb{Q}) = C_{p-1}$ eine (natürlich wieder zyklische) Untergruppe U der Ordnung n'. Sei

$$K = \mathrm{Fix}(U) = \{x \in \mathbb{Q}[\omega_p] \mid \sigma(x) = x \text{ für alle } \sigma \in U\}.$$

Die Galois-Theorie besagt: $[K\colon \mathbb{Q}] = n$.

8.5. Einheiten in $\mathbb{Q}[\omega_p]$

Satz. *Sei* p *ungerade Primzahl, sei* $\omega = \omega_p$ *eine primitive* p*-te Einheitswurzel und* $K = \mathbb{Q}[\omega]$.

(a) *Ist* η *eine Einheitswurzel in* K, *so ist* η *oder* $-\eta$ *eine* p*-te Einheitswurzel.*

(b) *Jede Einheit* $\eta \in \mathcal{O}_K$ *ist Produkt einer* p*-ten Einheitswurzel und einer reellen Einheit.*

Beweis. (a) Aufgabe 11.3.

(b) Mit η ist auch die komplex-konjugierte Zahl $\overline{\eta}$ in $\mathcal{O}_K$ und $\overline{\eta}$ ist ebenfalls eine Einheit in $\mathcal{O}_K$. Setze $\zeta = \eta\overline{\eta}^{-1}$. Behauptung: die zu ζ konjugierten Elemente ζ_i haben alle den Betrag 1. Sei $\sigma_a \in \mathrm{Gal}(\mathbb{Q}[\omega]\colon \mathbb{Q})$ durch $\sigma_a(\omega) = \omega^a$ definiert; insbesondere ist σ_{-1} die komplexe Konjugation, also ist $\zeta = \eta\sigma_{-1}(\eta)^{-1}$. und es gilt $\sigma_a\sigma_{-1} = \sigma_{-1}\sigma_a$ für alle a.

Es ist $\zeta_i = \sigma_a(\zeta)$ für ein $1 \leq a \leq p-1$. Also

$$\zeta_i = \sigma_a(\eta\sigma_{-1}(\eta)^{-1}) = \sigma_a(\eta) \cdot \sigma_a\sigma_{-1}(\eta)^{-1}) = \sigma_a(\eta) \cdot \sigma_{-1}\sigma_a(\eta)^{-1}) = \sigma_a(\eta) \cdot \overline{\sigma_a(\eta)}^{-1}.$$

Also ist

$$|\zeta_i = \sigma_a(\eta\sigma_{-1}(\eta)^{-1})| = |\sigma_a(\eta) \cdot \overline{\sigma_a(\eta)}^{-1}| = |\sigma_a(\eta)| \cdot |\overline{\sigma_a(\eta)}|^{-1} = 1$$

Es gilt ganz allgemein (siehe 8.6): Ist ζ eine Einheit, sodass alle Konjugierten von ζ den Betrag 1 haben, so ist ζ eine Einheitswurzel.

Natürlich gilt $\eta = \zeta\overline{\eta}$. Schreibe $\zeta = (\zeta')^2$ wobei auch ζ' eine p-te Einheitswurzel ist (dies ist möglich, denn p ist ungerade). Dann ist

$$\eta = \zeta\overline{\eta} = \zeta'(\zeta'\overline{\eta})$$

und

$$\overline{(\zeta'\overline{\eta})} = (\zeta')^{-1}\eta = \zeta'\overline{\eta},$$

also ist $\zeta'\overline{\eta}$ reell. Ist ζ eine p-te Einheitswurzel, so ist $\eta = \zeta'(\zeta'\overline{\eta})$ die gesuchte Faktorisierung. Ist dagegen $-\zeta$ eine n-te Einheitswurzel, so betrachtet man $\eta = (-\zeta')(-\zeta'\overline{\eta})$.

8.6. Nachtrag: Der Betrag einer ganzen algebraischen Zahl.

Satz. *Sei $c > 0$ eine reelle Zahl. Sei K algebraischer Zahlkörper. Es gibt nur endlich viele Zahlen $\alpha \in \mathcal{O}_K$ mit $|\alpha_i| \leq c$ für alle Konjugierten α_i von α.*

Beweis: Der Grad von K (über $\mathbb{Q}$) sei n. Setze

$$c' = \max\{1, \tbinom{n}{1}c, \tbinom{n}{2}c^2, \ldots, \tbinom{n}{n-1}c^{n-1}, c^n\}.$$

Sei $\alpha \in \mathcal{O}_K$ mit $|\alpha_i| \leq c$. Sei s_r das r-te elementar-symmetrische Polynom in n Variablen, also

$$s_r(X_1, \ldots, X_n) = \sum\nolimits_{i_1<i_2<\cdots<i_r} X_{i_1} \cdots X_{i_r},$$

beachte, dass dies eine Summe mit $\binom{n}{r}$ Summanden ist. Es ist

$$|s_r(\alpha_1, \ldots, \alpha_n)| \leq \tbinom{n}{r} \cdot c^r \leq c'.$$

Wir sehen also: Die Koeffizienten des Minimalpolynom f von α sind betragsmäßig durch c' beschränkt, also gehört f zur endlichen Menge

$$S = \Big\{ \sum_{i=0}^{n} b_i X \;\Big|\; |b_i| \leq c' \Big\} \subset \mathbb{Z}[T].$$

Da S endlich ist, ist auch die Anzahl der Nullstellen der Polynome in S endlich (jedes dieser Polynome hat nur endlich viele Nullstellen).

Bemerkung: In $\mathcal{O}_K$ kann es natürlich unendlich viele Zahlen α mit $|\alpha| \leq c$ geben. Betrachte etwa $K = \mathbb{Q}[\sqrt{2}]$ und $c = 1$. Es ist $|3 - 2\sqrt{2}| < 1$, also sind die Zahlen $(3 - 2\sqrt{2})^n$ mit $n \in \mathbb{N}_1$ paarweise verschieden und $|(3 - 2\sqrt{2})^n| < 1$.

Folgerung. *Sei K algebraischer Zahlkörper. Sei $\alpha \in \mathcal{O}_K$ mit $|\alpha_i| = 1$ für alle Konjugierten α_i von α. Dann ist α eine Einheitswurzel.*

Betrachte α^n mit $n \in \mathbb{N}_1$. Die Konjugierten von α^n sind $(\alpha^n)_i = (\alpha_i)^n$. Aus $|\alpha_i| = 1$ folgt

$$|(\alpha^n)_i| = |(\alpha_i)^n| = |\alpha_i|^n = 1.$$

Der Satz besagt: die Elemente $\alpha, \alpha^2, \alpha^3, \ldots$ sind nicht paarweise verschieden. Sei etwa $a < b$ mit $\alpha^a = \alpha^b$. Dann ist $\alpha^{b-a} = 1$, also ist α eine $(b-a)$-te Einheitswurzel.