Aufgabe 1 (Frühjahr 2009)**.** (a) Berechnen Sie das Minimalpolynom von $\zeta_{15} = e^{\frac{2\pi i}{15}}$ über $\mathbb{Q}$.

(b) Seien M der Zerfällungskörper von $X^{15} - 10$ über $\mathbb{Q}$ und G die Automorphismengruppe von M über $\mathbb{Q}$. Bestimmen Sie die Gruppe G und zeigen Sie, daß G nicht isomorph zur symmetrischen Gruppe S_5 ist.

Lösung. **Zu (a):** ζ_{15} ist eine primitive fünfzehnte Einheitswurzel. Sie ist Nullstelle des fünfzehnten Kreisteilungspolynoms, welches, wie alle Kreisteilungspolynome über $\mathbb{Q}$ irreduzibel ist. Also ist dies das Minimalpolynom von ζ_{15}. Es gilt

$$X^{15} - 1 = \phi_1 \cdot \phi_3 \cdot \phi_5 \cdot \phi_{15}.$$

Für die Primzahlen 3 und 5 gilt $\phi_3 = X^2 + X + 1$, $\phi_5 = X^4 + X^3 + X^2 + X + 1$, außerdem $\phi_1 = X - 1$, und weiter $\phi_3 \cdot \phi_1 = X^3 - 1$ und $\phi_5 \cdot \phi_1 = X^5 - 1$. Wir werden die letzte Gleichung benutzen. Damit gilt $X^{15} - 1 = \phi_{15} \cdot (X^2 + X + 1) \cdot (X^5 - 1)$ also

$$\begin{aligned}\phi_{15} &= \frac{X^{15} - 1}{(X^2 + X + 1) \cdot (X^5 - 1)} \\ &= \frac{X^{10} + X^5 + 1}{X^2 + X + 1}\end{aligned}$$

Da $\mathbb{Q}[X]$ ein euklidischer Ring ist, kann man dies mit Polynomdivision berechnen und erhält

$$(X^{10} + X^5 + 1) : (X^2 + X + 1) = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1$$

und dies ist ϕ_{15}.

Zu (b): Das Polynom $f = X^{15} - 10$ ist irreduzibel nach Eisenstein. Da $\mathbb{Q}$ Charakteristik 0 hat, also vollkommen ist, ist es auch separabel, hat also nur einfache Nullstellen. Also sein Zerfällungskörper M Galois'sch über $\mathbb{Q}$. Sei α eine Nullstelle von f, dann sind die weiteren Nullstellen gegeben durch $\zeta_{15}^n \alpha$ für $0 \leqslant n < 15$. Das irreduzible Polynom f ist Minimalpolynom von α. Da α und $\zeta_{15}\alpha \in M$, ist auch $\zeta_{15} = \frac{\zeta_{15}\alpha}{\alpha} \in M$. Also ist $M = \mathbb{Q}(\alpha, \zeta_{15})$. Nach der Gradformel gilt

$$[\mathbb{Q}(\alpha, \zeta_{15}) : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \zeta_{15}) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \zeta_{15}) : \mathbb{Q}(\zeta_{15})] \cdot [\mathbb{Q}(\zeta_{15}) : \mathbb{Q}].$$

Wir wissen bereits, daß

$$\begin{aligned}[\mathbb{Q}(\alpha) : \mathbb{Q}] &= \deg f = 15, \\ [\mathbb{Q}(\zeta_{15}) : \mathbb{Q}] &= \deg \phi_{15} = 8.\end{aligned}$$

Weiterhin ist das Minimalpolynom von ζ_{15} über $\mathbb{Q}(\alpha)$ ein Teiler von ϕ_{15}, also $[\mathbb{Q}(\alpha, \zeta_{15}) : \mathbb{Q}(\alpha)] \leqslant 8$ und das Minimalpolynom von α über $\mathbb{Q}(\zeta_{15})$ ein Teiler von f, also $[\mathbb{Q}(\alpha, \zeta_{15}) : \mathbb{Q}(\zeta_{15})] \leqslant 15$. Es gilt demnach

$$[\mathbb{Q}(\alpha, \zeta_{15}) : \mathbb{Q}(\alpha)] \cdot 15 = [\mathbb{Q}(\alpha, \zeta_{15}) : \mathbb{Q}(\zeta_{15})] \cdot 8.$$

Da 15 und 8 relativ prim sind, muß aber gelten $15 \big| [\mathbb{Q}(\alpha, \zeta_{15}) : \mathbb{Q}(\zeta_{15})]$ und $8 \big| [\mathbb{Q}(\alpha, \zeta_{15}) : \mathbb{Q}(\alpha)]$, also

$$[\mathbb{Q}(\alpha, \zeta_{15}) : \mathbb{Q}] = 15 \cdot 8 = 5 \cdot 3 \cdot 4 \cdot 2 = 5!.$$

Dies ist ebenfalls die Ordnung von S_5. Jedes Element $\sigma \in \mathrm{Gal}(\mathbb{Q}(\alpha, \zeta_{15})/\mathbb{Q})$ ist eindeutig durch $\sigma(\alpha)$ und $\sigma(\zeta_{15})$ bestimmt. Für den ersten Wert gibt es 15 Möglichkeiten - nämlich die 15 Nullstellen von f, also

$$\sigma(\alpha) = \zeta_{15}^k \alpha \quad \text{für ein } k \in \mathbb{Z}.$$

Für den zweiten Wert gibt es 8 Möglichkeiten - nämlich die primitiven fünfzehnten Einheitswurzeln, also

$$\sigma(\zeta_{15} = \zeta_{15}^l \quad \text{für ein } l \in \mathbb{Z} \text{ teilerfremd zu } 15.$$

Wir definieren eine Abbildung

$$\rho : \mathrm{Gal}(M/\mathbb{Q}) \to \mathbb{Z}/15\mathbb{Z} \times_j (\mathbb{Z}/15\mathbb{Z})^*, \sigma \mapsto (\overline{k}, \overline{l}),$$

wobei $j : (\mathbb{Z}/15\mathbb{Z})^* \to \mathrm{Aut}(\mathbb{Z}/15\mathbb{Z})$ gegeben ist durch $j(\overline{x})(\overline{y}) = \overline{xy}$. Beachte, daß k, l modulo 15 eindeutig bestimmt sind, also die Abbildung ρ wohldefiniert. Sie ist ein Gruppenhomomorphismus, denn für $\sigma_1, \sigma_2 \in \mathrm{Gal}(M/\mathbb{Q})$ mit $\sigma_i(\alpha) = \zeta_{15}^{k_i}\alpha$ und $\sigma_i(\zeta_{15}) = \zeta_{15}^{l_i}$ gilt

$$\sigma_1\sigma_2(\alpha) = \sigma_1(\zeta_{15}^{k_2}\alpha) = \sigma_1(\zeta_{15})^{k_2}\sigma_1(\alpha) = \zeta_{15}^{l_1k_2}\zeta_{15}^{k_1}\alpha = \zeta_{15}^{l_1k_2+k_1}\alpha$$
$$\sigma_1\sigma_2(\zeta_{15}) = \sigma(\zeta_{15}^{l_2}) = \zeta_{15}^{l_1l_2}$$

Also

$$\rho(\sigma_1\sigma_2) = (\overline{l_1k_2 + k_1}, \overline{l_1l_2}) = (\overline{k}_1 + j(\overline{k}_2)(\overline{l}_1), \overline{l}_1\overline{l}_2) = (\overline{k}_1, \overline{l}_1)(\overline{k}_2, \overline{l}_2).$$

Die Abbildung ist injektiv, denn aus $\rho(\sigma) = (\overline{0}, \overline{1})$ folgt $\sigma(\alpha) = \alpha$ und $\sigma(\zeta_{15}) = \zeta_{15}$, also $\sigma = \mathrm{id}$. Dies zeigt, daß $\mathrm{Gal}(M/\mathbb{Q})$ ein Element der Ordnung 15 hat. Obwohl G und S_5 die Gleiche Ordnung haben, können sie nicht isomorph sein, da S_5 kein Element der ORdnung 15 hat.

Aufgabe 2 (Herbst 2003)**.** Beweisen Sie:

$$\cos\frac{2\pi}{5} = \frac{\sqrt{5}-1}{4}.$$

Lösung. Es ist

$$\zeta_5 := e^{\frac{2\pi i}{5}} = \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5} \neq 1$$

primitive fünfte EInheitswurzel. Das fünfte Kreistielungspolanom ist

$$X^4 + X^3 + X^2 + X + 1$$

und es ist Minimalpolynom von ζ_5 über $\mathbb{Q}$.
Die Potenzen von ζ_5 bilden die Ecken einesin den Einheitskreid einbeschriebenen regulären Fünfecks. Die reelle Zahl $\cos\frac{2\pi}{5}$ liegt auf dem Schnittpunkt von ζ_5 und $\zeta_5^4 = \zeta_5^{-1}$ und der reellen Achse. Also

$$\cos\frac{2\pi}{5} = \frac{\zeta_5 + \zeta_5^4}{2}.$$

Wir sind also fertig, wenn wir zeigen, daß

$$\zeta_5 + \zeta_5^4 = \frac{\sqrt{5}-1}{2}.$$

Durch Zurückrechnen sieht man, daß $\frac{\sqrt{5}-1}{2}$ Nullstelle des Polynoms $f = X^2 + X - 1$ ist.
Es gilt

$$f(\zeta_5 + \zeta_5^4) = (\zeta_5 + \zeta_5^4)^2 + \zeta_5 + \zeta_5^4 - 1 = \zeta_5^2 + 2\zeta_5^5 + \zeta_5^8 + \zeta_5 + \zeta_5^4 - 1 = \zeta_5^2 + 1 + \zeta_5^3 + \zeta_5 + \zeta_5^4 = 0.$$

Also ist auch $\zeta_5 + \zeta_5^4$ eine Nullstelle. Und es muß $\zeta_5 + \zeta_5^4 = \frac{\sqrt{5}-1}{2}$ gelten, denn die zweite Nullstelle von f ist $\frac{-\sqrt{5}-1}{2} = -\frac{\sqrt{5}+1}{2} < 1$.

Aufgabe 3 (Frühjahr 2004)**.** Es sein $n > 2$ und ζ eine primitive n-te Einheitswurzel über $\mathbb{Q}$. Zeigen Sie:

$$[\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}] = \frac{1}{2}\varphi(n),$$

wobei φ die Euler'sche φ-Funktion bezeichnet.

Lösung. Es ist (aus der Wiederholung/Vorlesung) bekannt, daß $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$. Da offensichtlich $\zeta + \zeta^{-1} \in \mathbb{Q}(\zeta)$ ist der davon erzeugte Korper ein Zwischen körper

$$\mathbb{Q} \subset \mathbb{Q}(\zeta + \zeta^{-1}) \subset \mathbb{Q}(\zeta).$$

Also gilt nach dem Gradsatz

$$\varphi(n) = [\mathbb{Q}(\zeta) : \mathbb{Q}] = [\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})] \cdot [\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}].$$

Wir werden $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})]$ berechnen.
Zuerst überlegen wir uns, daß für $n > 2$ jede n-ten primitiven Einheitswurzel echt komplex ist, also $\zeta \in \mathbb{C} \setminus \mathbb{R}$. Das Inverse von ζ ist das komplex Konjugiert $\overline{\zeta}$, denn

$$1 = |\zeta|^2 = \zeta \cdot \overline{\zeta}.$$

Es folgt, daß $\zeta + \zeta^{-1} = \zeta + \overline{\zeta} = 2\mathrm{Re}s(\zeta) \in \mathbb{R}$. Also ist $\mathbb{Q}(\zeta) \neq \mathbb{Q}(\zeta + \zeta^{-1})$, das heißt $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})] \geqslant 2$.
Wir bestimmen nun das Minimalpolynom von ζ über $\mathbb{Q}(\zeta + \zeta^{-1})$. Wegen $\zeta(\zeta + \zeta^{-1}) = \zeta^2 + 1$ gilt

$$\zeta^2 - (\zeta + \zeta^{-1})\zeta + 1 = 0.$$

Also ist ζ Nullstelle des Polynoms $X^2 - (\zeta + \zeta^{-1})X + 1 \in \mathbb{Q}(\zeta + \zeta^{-1})[X]$. Somit gilt $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})] \leqslant 2$.
Es folgt $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})] = 2$, also

$$[\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}] = \frac{\varphi(n)}{2}$$

wie gewünscht.

Aufgabe 4 (Frühjahr 2004)**.** Für Primzahlpotenzen q bezeichne $\mathbb{F}_q$ den Körper aus q Elementen.

(a) Bestimmen Sie die kleinste Zweierpotenz $q = 2^m$, so daß der Körper $\mathbb{F}_q$ eine primitive 17-te Einheitswurzel enthält.

(b) Es sei α ein erzeugendes Element der multiplikativen Gruppe des Körpers $\mathbb{F}_{256}$. Welchen Grad hat das Minimalpolynom f von α über $\mathbb{F}_2$? Welche Potenzen von α sind Nullstellen von f?

(c) Es sei α wie in (b). Zeigen Sie unter Benutzung der Galois-Theorie, daß das Polynom

$$g(X) = (X - \alpha)(X - \alpha^4)(X - \alpha^{16})(X - \alpha^{64})$$

Koeffizienten in $\mathbb{F}_4$ hat.

Lösung. **Zu (a):** Da 17 prim ist, ist ein Element ζ genau dann eine primitiv siebzehnte Einheitswurzel, wenn $\zeta^{17} = 1$ und $\zeta \neq 1$. Ein solches Element existiert genau dann in $\mathbb{F}_q$, wenn

$$17 \big| |\mathbb{F}_q^*| = q - 1 = 2^m - 1.$$

Wir testen dies für "kleine" m:

$$\begin{aligned}
17 &\nmid 2^1 - 1 = 1 \\
17 &\nmid 2^2 - 1 = 3 \\
17 &\nmid 2^3 - 1 = 7 \\
17 &\nmid 2^4 - 1 = 15 \\
17 &\nmid 2^5 - 1 = 31 \\
17 &\nmid 2^6 - 1 = 63 \\
17 &\nmid 2^7 - 1 = 127 \\
17 &| 2^8 - 1 = 255 = 15 \cdot 17
\end{aligned}$$

Zu (b): Wir wissen, daß die multiplikative Gruppe eines endlichen Körpers zyklisch ist. Sei $\langle \alpha \rangle = \mathbb{F}_{256}^*$ ein Erzeuger. Es ist klar, daß α dann ein primitives Element der Erweiterung $\mathbb{F}_{256} / \mathbb{F}_2$ sein muß. Diese ht Grad 8, also hat das Minimalpolynom von α über $\mathbb{F}_2$ auch den Grad 8.
Es ist bekannt, daß $\mathbb{F}_{256} / \mathbb{F}_2$ als endliche Erweiterung eines endlichen Körpers Galois'sch ist und daß die Galoisgruppe zyklisch ist und vom Frobenius $\sigma : x \mapsto x^2$ erzeugt wird $\mathrm{Gal}(\mathbb{F}_{256} / \mathbb{F}_2) = \{\mathrm{id}, \sigma, \sigma^2, \ldots, \sigma^7\}$.

Da $\mathrm{Gal}(\mathbb{F}_{256}/\mathbb{F}_2)$ die Nullstellen von f permutiert, erhält man diese, indem man die Elemente der Galoisgruppe auf α anwendet:

$$\begin{aligned}\mathrm{id}(\alpha) &= \alpha\\ \sigma(\alpha) &= \alpha^2\\ \sigma^2(\alpha) &= \alpha^4\\ \sigma^3(\alpha) &= \alpha^8\\ \sigma^4(\alpha) &= \alpha^{16}\\ \sigma^5(\alpha) &= \alpha^{32}\\ \sigma^6(\alpha) &= \alpha^{64}\\ \sigma^7(\alpha) &= \alpha^{128}\end{aligned}$$

Zu (c): Die Zwischenkörper von $\mathbb{F}_{256}$ und $\mathbb{F}_2$ sind

$$\mathbb{F}_2 \subsetneq \mathbb{F}_4 \subsetneq \mathbb{F}_{16} \subsetneq \mathbb{F}_{256}\,.$$

Der Körper $\mathbb{F}_4$ hat Grad 2 über $\mathbb{F}_2$ und ist Fixkörper der Untergruppe $\{\mathrm{id}, \sigma^2, \sigma^4, \sigma^6\} = \langle\sigma^2\rangle$ vom Index 2 in $\mathrm{Gal}(\mathbb{F}_{256}/\mathbb{F}_2)$. Es gilt

$$\begin{aligned}\sigma^2(\alpha) &= \alpha^4\\ \sigma^2(\alpha^4) &= \alpha^{16}\\ \sigma^2(\alpha^{16}) &= \alpha^{64}\\ \sigma^2/\alpha^{64} &= \alpha\end{aligned}$$

Daher ist $\alpha^2(g) = g$, und die Koeffizienten von g müssen in $\mathbb{F}_4$ sein.

Aufgabe 5 (Frühjahr 1998)**.** Es sei $f(X) \in \mathbb{Q}[X]$ irreduzibel von ungeradem Grad m. Sei ω eine primitive siebzehnte Einheitswurzel. Zeigen Sie, daß $f(X)$ über $\mathbb{Q}(\omega)$ irreduzibel ist.

Lösung. Weil f irreduzibel ist, ist das davon erzeugte Ideal (f) ein Primideal, und damit ein maximales Ideal in dem Hauptidealring $\mathbb{Q}[X]$. Es folgt, daß $\mathbb{Q}[X]/(f)$ ein Körper ist. Ist α eine Nullstelle von f in einem Zerfällungskörper, so ist

$$\mathbb{Q}[X]/(f) \to \mathbb{Q}(\alpha), X + (f) \mapsto \alpha$$

ein Isomorphismus, f ist das Minimalpolynom von α über $\mathbb{Q}$, und $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg f = m$.
Wir untersuchen nun α über dem Kreisteilungskörper $\mathbb{Q}(\omega)$. Da ω siebzehnte Einheitswurzel ist, ist $[\mathbb{Q}(\omega) : QQ] = \deg \Phi_1 7 = \varphi(17) = 16 = 2^4$.
Sei g das Minimalpolynom von α über $\mathbb{Q}(\omega)$. Da α Nullstelle des Polynoms $f \in \mathbb{Q}[X] \subset \mathbb{Q}(\omega)[X]$ ist, muß $g \big| f$. Also $\deg g \leqslant \deg f$, und es gilt $[\mathbb{Q}(\omega, \alpha) : \mathbb{Q}(\omega)] = \deg g \leqslant m$.
Genauso teilt das Minimalpolynome von ω über $\mathbb{Q}(\alpha)$ des siebzehnte Kreisteilungspolynom und $[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\alpha)] \leqslant 16$.
Die Gradformel ergibt

$$[\mathbb{Q}(\alpha,\omega) : \mathbb{Q}(\alpha)]\cdot m = [\mathbb{Q}(\alpha,\omega) : \mathbb{Q}(\alpha)]\cdot[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\omega,\alpha) : \mathbb{Q}] = [\mathbb{Q}(\omega,\alpha) : \mathbb{Q}(\omega)]\cdot[\mathbb{Q}(\omega) : QQ] = [\mathbb{Q}(\omega,\alpha) : \mathbb{Q}(\omega)]\cdot 16$$

Da m und 16 teilerfremd sind gilt

$$m \big| [\mathbb{Q}(\omega,\alpha) : \mathbb{Q}(\omega)] \leqslant m.$$

Es folgt $g = f$, also ist f irreduzibel über $\mathbb{Q}(\omega)$.