Aufgabe 1. Zeige, daß die folgenden Polynome irreduzibel über $\mathbb{Q}$ sind:

i) $f = X^{10} + 2X^8 + 4X^6 + 6X^4 + 8X^2 + 10$. *(3 Punkte)*
ii) $g = X^4 + 3X^3 + 5X^2 + 7X + 9$. *(3 Punkte)*

Für i) funktioniert Eisenstein mit $p = 2$. Für ii) empfehle ich Reduktion nach $\mathbb{Z}/2\mathbb{Z}[X]$: Das Polynom hat keine Nullstellen in $\mathbb{Z}/2\mathbb{Z}$ (ausprobieren!), also müssen wir nur Zerlegbarkeit in zwei irreduzible normierte Faktoren vom Grad 2 ausschließen. Aber es gibt überhaupt nur ein irreduzibles normiertes Polynom vom Grad 2 in $\mathbb{Z}/2\mathbb{Z}[X]$, nämlich $X^2 + X + 1$ (die anderen, $X^2 + 1$, $X^2 + X$ und X^2, haben Nullstellen), und dessen Quadrat ist $X^4 + X^2 + 1 \neq \overline{g}$.

Aufgabe 2. Es sei L der Zerfällungskörper des Polynoms $X^3 - 5$ über $\mathbb{Q}$. Bestimme alle Zwischenkörper der Erweiterung $\mathbb{Q} \subset L$. *(6 Punkte)*

Es ist $L = \mathbb{Q}(a, \zeta)$ mit $a = \sqrt[3]{5}$ und $\zeta = \exp(2\pi i/3)$. Wegen $L \not\subset \mathbb{R}$, aber $\mathbb{Q}(a) \subset \mathbb{R}$, muß $L \neq \mathbb{Q}(a)$ sein, und nach der Gradformel erhalten wir daraus $[L : \mathbb{Q}] = 6$. Die Galoisgruppe ist also isomorph zu einer 6-elementigen Untergruppe der Permutationsgruppe der Nullstellenmenge $\{a, a\zeta, a\zeta^2\}$, also isomorph zur S_3.
Die S_3 hat nun folgende Untergruppen: Jeweils eine triviale mit einem bzw. 6 Elementen, eine einzige Untergruppe der Ordnung 3 (zum Beispiel nach Sylowtheorie) und die drei Untergruppen der Ordnung 2, erzeugt von $(1\ 2)$, $(1\ 3)$ bzw. $(2\ 3)$. (Daß das alle sind, sieht man beispielsweise auch mit Sylowtheorie).
Nach dem Hauptsatz der Galoistheorie müssen wir also außer den trivialen Zwischenkörpern $\mathbb{Q}$ und L genau einen vom Grad 2 und drei verschiedene vom Grad 3 finden. Nun hat $\mathbb{Q}(\zeta)$ Grad 2 über $\mathbb{Q}$, und die von jeweils einer Nullstelle erzeugten Zwischenkörper $\mathbb{Q}(a)$, $\mathbb{Q}(a\zeta)$, $\mathbb{Q}(a\zeta^2)$ haben Grad 3 über $\mathbb{Q}$. Sie sind auch alle verschieden, denn wären zwei von ihnen gleich, so enthielten beide auch das Element ζ und wären damit gleich L.

Aufgabe 3. Zeige, daß jede Gruppe der Ordnung 70 auflösbar ist. *(6 Punkte)*

Es ist $70 = 2 \cdot 5 \cdot 7$. Die Anzahl s_5 der 5-Sylowuntergruppen ist ein Teiler von 14, der $\equiv 1 \pmod 5$ ist, also muß $s_5 = 1$ sein. Also enthält die Gruppe einen (auflösbaren!) Normalteiler der Ordnung 5, und wir müssen nur zeigen, daß jede Gruppe der Ordnung $70/5 = 14$ auflösbar ist. Wieder nach Sylowtheorie enthält diese aber einen (auflösbaren!) Normalteiler der Ordnung 7, und der Quotient ist als Gruppe der Ordnung 2 wieder auflösbar.

Aufgabe 4.

i) Finde einen Unterkörper $K \subset \mathbb{C}$ mit $[K : \mathbb{Q}] = 4$, so daß $K/\mathbb{Q}$ nicht galoissch ist. *(3 Punkte)*
ii) Finde einen Unterkörper $L \subset \mathbb{C}$ mit $[L : \mathbb{Q}] = 4$, so daß $L/\mathbb{Q}$ galoissch ist. *(3 Punkte)*

Für i) nimm etwa $K = \mathbb{Q}(\sqrt[4]{2})$. Diese Erweiterung ist nicht normal, da das Minimalpolynom von $\sqrt[4]{2}$, also $X^4 - 2$, zwar eine Nullstelle in K besitzt, in K jedoch nicht zerfällt: denn K läßt sich in $\mathbb{R}$ einbetten, aber nicht einmal in $\mathbb{R}$ zerfällt das Polynom (es hat genau zwei reelle Nullstellen, und diese sind einfach).
Für ii) tut es beispielsweise $L = \mathbb{Q}(i, \sqrt{2})$. Man sieht $[L : \mathbb{Q}] = 4$ mit dem Gradsatz (wegen $i \notin \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$), und L ist Zerfällungskörper des Polynoms $(X^2 + 1)(X^2 - 2) \in \mathbb{Q}[X]$, also eine Galoiserweiterung von $\mathbb{Q}$.

Aufgabe 5. Es sei K ein Körper und $f \in K[X]$ irreduzibel mit Zerfällungskörper L über K. Es sei $a \in L$ eine Nullstelle von f. Zeige, daß $L = K(a)$ ist, wenn eine der folgenden Voraussetzungen vorliegt:

i) Das Polynom f ist separabel, und $\mathrm{Gal}(L/K)$ ist abelsch. *(4 Punkte)*
ii) Der Körper K ist endlich. *(2 Punkte)*

Für i) genügt es zu zeigen, daß $K(a)/K$ normal ist: denn dann zerfällt f in $K(a)$, also folgt $L \subset K(a)$ und damit $L = K(a)$. Aber L/K ist galoissch, und da jede Untergruppe einer abelschen Gruppe normal ist, ist *jeder* Zwischenkörper galoissch und insbesondere normal über K.
ii) ist eine direkte Anwendung von i), denn jedes irreduzible Polynom über einem endlichen Körper ist separabel, und jede Erweiterung endlicher Körper ist galoissch mit sogar zyklischer Galoisgruppe (erzeugt vom Frobeniushomomorphismus).

Zusatzaufgabe. Zeige, daß jede Gruppe der Ordnung 33 zyklisch ist. *(6 Extrapunkte)*

Sylowtheorie zeigt, daß eine Gruppe G mit $|G| = 33$ zwei Normalteiler P, Q mit $|P| = 3$, $|Q| = 11$ besitzt. Ich behaupte, daß $i : P \times Q \to G$, $(p,q) \to pq$, ein Gruppenisomorphismus ist. Zunächst ist $P \cap Q = \{e\}$ (denn $|P \cap Q|$ teilt nach Lagrange sowohl 3 als auch 11). Daraus folgt, daß Elemente von P mit Elementen von Q vertauschen: Ist nämlich $p \in P$, $q \in Q$, so ist $[p,q] = pqp^{-1}q^{-1}$ wegen $pqp^{-1} \in Q$ ein Element von Q und gleichzeitig wegen $qp^{-1}q^{-1} \in P$ ein Element von P, also trivial, d.h. $pq = qp$. Damit folgt nun mühelos, daß i ein Homomorphismus ist. Der Kern von i ist trivial, wenn aus $pq = e$ folgt $p = q^{-1} \in P \cap Q = \{e\}$, also $p = q$. Also ist i injektiv und wegen $|P \times Q| = |G|$ auch surjektiv. Aber wegen $P \cong \mathbb{Z}/3\mathbb{Z}$ und $Q \cong \mathbb{Z}/11\mathbb{Z}$ (Klassifikation der Gruppen von Primzahlordnung) haben wir damit $G \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z} \cong \mathbb{Z}/33\mathbb{Z}$ nach dem chinesischen Restsatz, d.h. G ist zyklisch.
Eine andere mögliche Argumentation ist die folgende: Da 33 nur die Teiler $1, 3, 11, 33$ hat, hat jedes Element der Gruppe eine dieser Zahlen als Ordnung. Da es aber nur jeweils eine 3- bzw. 11-elementige Untergruppe gibt (Sylowsätze), haben wir nur $1 + 2 + 10 = 13$ Elemente der Ordnung $\leqslant 11$. Also gibt es Elemente der Ordnung 33, d.h. G ist zyklisch.

(Extraplatz zum Weiterschreiben)

(Extraplatz zum Weiterschreiben)