Aufgabe 1: (20 Punkte) Nach Voraussetzung ist $(G, \cdot)$ eine Gruppe. Wir geben eine Abbildung $\varphi_x : (G, \odot) \to (G, \cdot)$ an, vermöge $\varphi_x(a) \mapsto xa$. Dann gilt:

$$\varphi_x(a \odot b) = \varphi_x(axb) = xaxb = \varphi_x(a) \cdot \varphi_x(b).$$

Die Abbildung ist ein Homomorphismus zwischen den beiden Gruppen. Desweiteren ist die Abbildung eine Bijektion (mit x aus der Gruppe G ist auch $x^{-1} \in G$), damit ein Gruppenisomorphismus. (Aufgrund der Isomorphie zu der Gruppe $(G, \cdot)$ haben wir auch gezeigt, dass $(G, \odot)$ selbst eine Gruppe ist.)

(In $(G, \odot)$ ist x^{-1} (und nicht 0 oder 1 wie einige geschrieben haben) das neutrale Element. Deswegen ist das inverse Element zu a bzgl. der Verknüpfung $\odot$ das Element $a' := x^{-1}a^{-1}x^{-1}$, wegen $a \odot a' = axx^{-1}a^{-1}x^{-1} = a1_{(G,\cdot)}a^{-1}x^{-1} = x^{-1}$. Rechts steht das neutrale Element bzgl. $\odot$.)

Aufgabe 2: (20 Punkte) Für eine Einheit $a + b\sqrt{3}$ des Ringes muss gelten $1 = \mathrm{N}(1) = \mathrm{N}(a + b\sqrt{3}) = a^2 - 3b^2$. (Das war der Hinweis in der Aufgabenstellung, den Ihr hättet benutzen sollen. Wenn Ihr eine Seite rumrechnet, nur um diesen Hinweis neu zu entdecken, ist es nicht verwunderlich, dass Euch die Zeit davonläuft.)

Eine Lösung ist z.B. $\zeta := 2+1\sqrt{3}$. Mit $\zeta^{-1} = 2-\sqrt{3}$ haben wir die Beziehung $1 = \zeta\zeta^{-1}$. Wegen $1 = 1^n = \zeta^n\zeta^{-n}$ finden wir bereits unendlich viele weitere Einheiten als Potenzen von ζ.

Aufgabe 3: (16 Punkte) Wir argumentieren wieder über die Norm. Wäre $\alpha := 9 - 2\sqrt{17}$ reduzibel, also z.B. $\alpha = \beta\gamma$ für zwei Nicht-Einheiten β, γ, so würde für die Normen gelten

$$\mathrm{N}(\beta)\,\mathrm{N}(\gamma) = \mathrm{N}(\alpha) = 81 - 4 \cdot 17 = 13.$$

Rechts steht eine **Primzahl**[1]. D.h. es ist entweder $\mathrm{N}(\beta) = \pm 1$ oder $\mathrm{N}(\gamma) = \pm 1$, was nichts anderes bedeutet, als dass eine von beiden eine Einheit ist.

Damit ist die Zerlegung von α in Nicht-Einheiten unmöglich, α ist irreduzibel.

[1] Ja, 13 ist prim. Das ist ein Stichwort, das in einer Lösung hätte vorkommen dürfen, es erleichtert die weitere Argumentation ungemein.

Aufgabe 4: (24 Punkte) Diese Aufgabe ist der Beweis zu Satz 4.9 (b) in Kapitel 6 im Artin.

Hinweise zu einzelnen Teilaufgaben:
Zu 2.: Wir wissen, dass alle p-Sylowgruppen zueinander konjugiert sind. Es gilt also yKy^{-1} ist eine 7-Sylowgruppe. Wir haben im vorigen Aufgabenteil gezeigt, dass es nur eine einzige 7-Sylowgruppe gibt. Also ist $yKy^{-1} = K$. Für ein Element $x \in K$ bedeutet das, dass $yxy^{-1} \in K = \langle x \rangle = \left\{ x^i \,\middle|\, i = 0, \dots, 6 \right\}$ gilt. x^0 kann nicht sein, da yxy^{-1} und x^i die gleiche Ordnung haben müssen, da Konjugation u.a. die Ordnung erhält.

Zu 3.: Aus der Aufgabenstellung folgt sofort: $yx = x^i y$. Für $i \neq 1$ ist G **nicht** kommutativ. Es ist $y^3 = 1 = y^{-3}$. Damit ist $x = y^3xy^{-3} = y^2x^iy^{-2}$. Wenn wir nun ein y nach rechts wandern lassen müssen wir es mit dem ersten x von x^i vertauschen. Dadurch handeln wir uns ein x^i ein:

$$\begin{aligned} y^2x^iy^{-2} &= yyxx^{i-1}y^{-1}y^{-1} = yx^iyx^{i-1}y^{-1}y^{-1} = \dots \\ &= y(x^i)^{i-1}yxy^{-1}y^{-1} = y(x^i)^{i-1}x^iyy^{-1}y^{-1} = y(x^i)^iy^{-1} \\ &= yx^{i^2}y^{-1} = x^iyx^{i^2-1}y^{-1} = \dots = (x^i)^{i^2}yy^{-1} = x^{i^3} \end{aligned}$$

Zu 6.: Wir wenden wieder den Trick von 3. an: Vertauschen von yx erzeugt x^iy, mit $i = 4$. Desweiteren ist zu beachten, dass 7 die Ordnung von x ist. Deswegen gilt $x^{16} = x^{14}x^2 = 1^2 \cdot x^2 = x^2$.

$$\begin{aligned} z^2xz^{-1} &= y^2xy^{-2} = yyxy^{-2} = yx^4yy^{-1}y^{-1} = yxx^3y^{-1} \\ &= x^4yx^3y^{-1} = \dots = (x^4)^4yy^{-1} = x^{16} = x^2 \end{aligned}$$

Aufgabe 5: (20 Punkte) Wir bestimmen die Galoisgruppe G in mehreren Schritten:

1. Nach einem Satz der Vorlesung hat die Körpererweiterung den Grad n. Deswegen gilt $\#G \leq n$.
2. Desweiteren sei $\sigma : \mathbb{F}_q \to \mathbb{F}_q$, die Abbildung $\sigma(x) = x^p$. Wegen $x^p = x$ für alle $x \in \mathbb{F}_p$, ist σ die Identität auf $\mathbb{F}_p$. Es ist $\sigma(\sum_{k=0}^{n-1} a_k x^k) = \sum_{k=0}^{n-1} a_k \sigma(x^k) = \sum_{k=0}^{n-1} a_k (x^p)^k$. Nach einem Satz der Vorlesung ist σ ein Körperautomorphismus.

3. Weil $\mathbb{F}_q$ die Ordnung p^n hat, gilt $x^{p^n} = x$. Deswegen ist σ^n die Identität auf $\mathbb{F}_q$ und n ist die Ordnung von σ.

   Die n verschiedenen Abbildungen $\sigma, \sigma^2, \ldots, \sigma^n$ sind alle Elemente der Galoisgruppe. Da diese höchstens n Elemente enthält, haben wir die Galoisgruppe damit vollständig bestimmt.

Es ist $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) = \left\{\sigma^k \,\middle|\, k = 1, \ldots, n\right\}$.