**Universität Konstanz**
**Fachbereich Mathematik und Statistik**
**Wintersemester 2010/2011**

Dr. Andrew Dolphin
Prof. Dr. Markus Schweighofer

# Übungsblatt 14 zur Einführung in die Algebra: Solutions

**Aufgabe 1.** Sei $K$ ein Körper der Charakteristik $p > 0$, so dass der Frobenius-Homorphismus $\Phi_p : K \to K$ kein Automorphismus ist. Sei $a \in K \setminus \Phi_p(K)$. Zeige, dass $X^p - a \in K[X]$ irreduzibel und nicht separabel ist.

*Solution*

Since $f' = pX^{p-1} = 0$, we have clearly that $f$ is not separable. It remains we show irreducibility of $f := X^p - a$ in $K[X]$. Obviously, $f \notin K^\times = K[X]^\times$. Now let $f = X^p - a$, and suppose that $f = gh$, where $g,h \in K[X]$ are monic. We show that $g = 1$ or $h = 1$. Choosing $b \in \overline{K}$ with $b^p = a$, we have $f = (X^p - a) = (X^p - b^p) = (X - b)^p$ since $\operatorname{char} K[X] = \operatorname{char} K = p \in \mathbb{P}$. Using that $K[X]$ is factorial, we get $g = (X - b)^i$ and $h = (X - b)^j$ for some $i,j \in \mathbb{N}_0$ such that $i + j = p$. We have to show that $i = 0$ or $j = 0$, i.e. $i \in \{0,p\}$. It suffices to show that $(i,p) = (p)$. But since $p$ is prime, the only other possibility would be $(i,p) = 1$. In that case however, we would find $s,t \in \mathbb{Z}$ with $1 = si + tp$ leading to $b = b^{si+tp} = (b^i)^s(b^p)^t = (b^i)^s a^t \in K$ (since $g,f \in K[X]$), which is a contradiction to $a \notin \Phi_p(K)$.

**Aufgabe 2.** Sei $x \in \mathbb{R}$ mit $x^4 = 2$ und $L = \mathbb{Q}(\mathbb{i},x)$. Finde alle Zwischenkörper von $L|\mathbb{Q}$.

*Solution*

Let $f = X^4 - 2 \in \mathbb{Q}[X]$. Obviously

$$a_1 := \sqrt[4]{2}, \qquad a_2 := -\sqrt[4]{2}, \qquad a_3 := \mathbb{i}\sqrt[4]{2} \qquad \text{and} \qquad a_4 := -\mathbb{i}\sqrt[4]{2}$$

are the pairwise distinct zeros of $f$ in $\mathbb{C}$. The splitting field of $f$ over $\mathbb{Q}$ is therefore $\mathbb{Q}(a_1,a_2,a_3,a_4) = \mathbb{Q}(\mathbb{i},\sqrt[4]{2}) = \mathbb{Q}(\mathbb{i},x) = L$. In particular, $L|\mathbb{Q}$ is normal and therefore a Galois extension (since $\operatorname{char}\mathbb{Q} = 0$).

We now determine $[L : \mathbb{Q}]$. Since $f$ is irreducible over $\mathbb{Q} = \operatorname{qf}(\mathbb{Z})$ by Eisenstein, we have $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$. The minimum polynomial of $\mathbb{i}$ over $\mathbb{Q}(\sqrt[4]{2})$ is $X^2 + 1$, since $\mathbb{i} \notin \mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{R}$. So $[\mathbb{Q}(\mathbb{i},\sqrt[4]{2}) : \mathbb{Q}(\sqrt[4]{2})] = 2$. Hence $[\mathbb{Q}(\mathbb{i},\sqrt[4]{2}) : \mathbb{Q}] = [\mathbb{Q}(\mathbb{i},\sqrt[4]{2}) : \mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 2 \cdot 4 = 8$, and hence $\#\operatorname{Aut}(\mathbb{Q}(\mathbb{i},\sqrt[4]{2})|\mathbb{Q}) = [\mathbb{Q}(\mathbb{i},\sqrt[4]{2}) : \mathbb{Q}] = 8$.

Let $G := \operatorname{Aut}(\mathbb{Q}(\mathbb{i},\sqrt[4]{2})|\mathbb{Q}) \subseteq S_4$. We have $(3\ 4) \in G$ (as $\overline{a_1} = a_1$, $\overline{a_2} = a_2$ and $\overline{a_3} = a_4$ under complex conjugation). Since $f$ is irreducible in $\mathbb{Q}[X]$ (and therefore each two zeros of $f$ are conjugated over $\mathbb{Q}$) there is also $\varphi \in G$ with $\varphi(\sqrt[4]{2}) = \mathbb{i}\sqrt[4]{2}$. Then $\varphi(a_3) = \varphi(\mathbb{i}\sqrt[4]{2}) = \varphi(\mathbb{i})\varphi(\sqrt[4]{2}) = (\pm\mathbb{i})(\mathbb{i}\sqrt[4]{2}) = \mp\sqrt[4]{2} \in \{a_1,a_2\}$ and hence at least one of $(1\ 3)(2\ 4)$ and $(1\ 3\ 2\ 4)$ lies in $G$. Since the product of these two permutations is $(3\ 4)$ which is already known to lie in $G$, it follows that actually both of these permutations lie in $G$. Products of the three already found permutations yield

$$\{1,\ (1\ 2),\ (3\ 4),\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3),\ (1\ 3\ 2\ 4),\ (1\ 4\ 2\ 3)\}.$$

We know $\#G = 8$, and hence this set is the whole Galois group.

The different subgroups of $G$ are:

- $\langle 1 \rangle$ (order 1);
- $\langle (1\ 2) \rangle$, $\langle (3\ 4) \rangle$, $\langle (1\ 2)(3\ 4) \rangle$, $\langle (1\ 3)(2\ 4) \rangle$, $\langle (1\ 4)(2\ 3) \rangle$ (order 2);

- $\langle(1\ 3\ 2\ 4)\rangle$, $\langle(1\ 4\ 3\ 2)\rangle$, $\langle(1\ 2),(3\ 4)\rangle$ (order 4);
- $G$ (order 8).

**Intermediate fields of degree 1 over $\mathbb{Q}$:**

- The fixed field of the subgroup of order 8 is $\mathbb{Q}$.

**Intermediate fields of degree 2 over $\mathbb{Q}$:** The subgroups of order 4 have index 2 in $G$. Hence their fixed fields have degree 2 over $L^G = \mathbb{Q}$.

- Setting $\varphi := (1\ 3\ 2\ 4)$,
$$\varphi(\mathbb{i}) = \varphi(\frac{a_3}{a_1}) = \frac{\varphi(a_3)}{\varphi(a_1)} = \frac{a_2}{a_3} = -\frac{1}{\mathbb{i}} = \mathbb{i},$$
shows that the fixed field of $\langle(1\ 3\ 2\ 4)\rangle$ is $\mathbb{Q}(\mathbb{i})$.
- Similarly, setting $\varphi := (1\ 4\ 3\ 2)$,
$$\varphi(\sqrt{2}\mathbb{i}) = -\varphi(a_1a_3) = \varphi(a_1)\varphi(a_3) = a_4a_2 = \mathbb{i}\sqrt{2} = \sqrt{2}\mathbb{i}$$
shows that the fixed field of $\langle(1\ 3\ 2\ 4)\rangle$ is $\mathbb{Q}(\sqrt{2}\mathbb{i})$.
- Finally, setting $\varphi := (1\ 2)(3\ 4)$,
$$\varphi(\sqrt{2}) = \varphi(-a_1a_2) = -\varphi(a_1)\varphi(a_2) = -a_2a_1 = \sqrt{2}$$
shows that the fixed field of $\langle(1\ 2)(3\ 4)\rangle$ is $\mathbb{Q}(\sqrt{2})$.

**Intermediate fields of degree 4 over $\mathbb{Q}$:**
The subgroups of order 2 have index 4 in $G$. Hence their fixed fields have degree 4 over $L^G = \mathbb{Q}$.

- Obviously $a_3$ lies in the fixed field of $\langle(1\ 2)\rangle$. But since $[\mathbb{Q}(a_3):\mathbb{Q}] = 4$ by the irreducibility of $f$, we have that the fixed field of $\langle(1\ 2)\rangle$ actually equals $\mathbb{Q}(a_3) = \mathbb{Q}(\mathbb{i}\sqrt[4]{2})$.
- Analogously, the fixed field of $\langle(3\ 4)\rangle$ is $\mathbb{Q}(a_1) = \mathbb{Q}(\sqrt[4]{2})$.
- To determine the fixed field of $\langle(1\ 2)(3\ 4)\rangle$, we note that $\sqrt{2} = -a_1a_2$ and $\mathbb{i} = \frac{a_3}{a_1}$ lie in it. Now since $[\mathbb{Q}(\sqrt{2},\mathbb{i}):\mathbb{Q}] = 4$, we have that it actually equals $\mathbb{Q}(\sqrt{2},\mathbb{i})$.
- To determine the fixed field of $\langle(1\ 3)(2\ 4)\rangle$, we note that $(1+\mathbb{i})\sqrt[4]{2} = a_1 + a_3$ lies in it. To see that the fixed field equals $\mathbb{Q}((1+\mathbb{i})\sqrt[4]{2})$, we have however to show that $[\mathbb{Q}((1+\mathbb{i})\sqrt[4]{2}):\mathbb{Q}] = 4$. One way to do this, is to verify that $(1+\mathbb{i})\sqrt[4]{2}$ is a zero of $X^4+8$ and $X^4+8$ is irreducible over $\mathbb{Q}$. That $X^4+8$ is irreducible over $\mathbb{Q}$ can be checked by direct computation (assume $X^4+8$ factors and get a contradiction).
- To determine the fixed field of $\langle(1\ 4)(2\ 3)\rangle$, we note that $(1-\mathbb{i})\sqrt[4]{2} = a_1 + a_4$ lies in it. Since this is the complex conjugate of $(1+\mathbb{i})\sqrt[4]{2}$, it follows from the above that the fixed field actually equals $\mathbb{Q}((1-\mathbb{i})\sqrt[4]{2})$.

**Intermediate fields of degree 8 over $\mathbb{Q}$:**

- The fixed field of the subgroup of order 1 is $L = \mathbb{Q}(\mathbb{i}, \sqrt[4]{2})$.

**Resume:** The different intermediate fields of $L|\mathbb{Q}$ (and therefore the subfields of $L$) are

$\mathbb{Q}$, $\mathbb{Q}(\mathbb{i})$, $\mathbb{Q}(\sqrt{2}\mathbb{i})$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\mathbb{i}\sqrt[4]{2})$, $\mathbb{Q}(\sqrt[4]{2})$, $\mathbb{Q}(\sqrt{2},\mathbb{i})$, $\mathbb{Q}((1+\mathbb{i})\sqrt[4]{2})$, $\mathbb{Q}((1-\mathbb{i})\sqrt[4]{2})$ and $\mathbb{Q}(\mathbb{i},\sqrt[4]{2})$.

**Aufgabe 3.** Sei $K(x)|K$ eine algebraische Körpererweiterung von ungeradem Grad. Zeige $K(x^2) = K(x)$.

*Solution*

Clearly $x$ is a root of $X^2 - x^2 \in K(x^2)[X]$, hence $[K(x) : K(x^2)] \leqslant 2$. By the tower law we have that

$$[K(x) : K] = [K(x) : K(x^2)] \cdot [K(x^2) : K],$$

which is odd by hypothesis. Therefore $[K(x) : K(x^2)] = 1$.

**Aufgabe 4.**

(i) Zeige, dass die Galoisgruppe des Zerfällungskörpers eines irreduziblen separablen Polynoms vom Grad 3 über einem Körper isomorph zu $S_3$ oder $C_3$ ist

(ii) Bestimme die Galoisgruppe des Zerfällungskörpers von $X^3 - X - 1$ über $\mathbb{Q}$.

*Solution*

(i) Let $K$ be a field and let $f \in K[X]$ be an irreducible polynomial of degree 3. Let $L$ be a splitting field of $L$. $L|K$ is normal and separable, and $[L : K] = |\mathrm{Aut}(L|K)| \leqslant 6$ and $\mathrm{Aut}(L|K) \subseteq S_3$.

Let $a$,$b$,$c$ be the roots of $f$ in $L$. Since $f$ is irreducible, we have that $[K(a) : K] = 3$. Hence we have a tower of fields $K \subseteq K(a) \subseteq L$ with $[L : K] \leqslant 6$ and $[K(a) : K] = 3$. By the tower law we have $[L : K(a)] = 1$ or 2. We consider both cases.

If $[L : K(a)] = 2$, then $[L : K] = 6$, and so $\mathrm{Aut}(L|K)$ has 6 elements. But $\mathrm{Aut}(L|K) \subseteq S_3$ and $|S_3| = 6$, hence $\mathrm{Aut}(L|K) = S_3$.

If $[L : K(a)] = 1$, then $[L : K] = 3$ and $\mathrm{Aut}(L|K)$ has 3 elements. However, there is only one group of order 3, up to isomorphism, and that is $C_3$.

(ii) Let $f = X^3 - X - 1 \in \mathbb{Q}[X]$ and $L$ be a splitting field of $f$ over $\mathbb{Q}$. Since the characteristic of $\mathbb{Q}$ is 0, the extension $L|\mathbb{Q}$ is separable. We now show that $f$ is irreducible. If not, $f$ having the degree 3, it would have a zero $\frac{a}{b} \in \mathbb{Q}$ with $a$,$b \in \mathbb{Q} \setminus \{0\}$. We can assume without loss of generality that $(a,b) = (1)$ in $\mathbb{Z}$. Since $f(\frac{a}{b}) = 0$ it follows that $a^3 - ab^2 - b^3 = 0$, and hence that $a^3 = b^2(a + b)$. Let $p$ be a prime number such that $p|a$. Then $p$ must divide $a + b$ and therefore $b$, a contradiction. Hence $a = \pm 1$. Let $q$ be a prime number with $q|b$. Then it follows that $q|a$, again a contradiction, hence $b = \pm 1$. Therefore $\frac{a}{b} = \pm 1$, but $f(\pm 1) \neq 0$, and hence $f$ must be irreducible.

We now find the zeros of $f$. We know that $f$ has at least one real zero, $x_1$, as it is a polynomial of odd degree. Since $f' = 3X^2 - 1$, we see that $f$ is increasing in the range $(-\infty, -\sqrt{\frac{1}{3}}]$, decreasing in the range $[-\sqrt{\frac{1}{3}}, \sqrt{\frac{1}{3}}]$ and increasing again in the range $[\sqrt{\frac{1}{3}}, \infty)$. We also have that $f(-\sqrt{\frac{1}{3}}) < 0$, and hence $f$ has only one real zero, $x_1$. The two other zeros, $x_2$ and $x_3$ must be in $\mathbb{C} \backslash \mathbb{R}$. In particular we have

$$\mathbb{Q} \subsetneq \mathbb{Q}(x_1) \subsetneq \mathbb{Q}(x_1, x_2, x_3),$$

where $\mathbb{Q}(x_1,x_2,x_3)$ is the splitting field of $f$.

Since $f$ is irreducible over $\mathbb{Q}$, we have that $[\mathbb{Q}(x_1) : \mathbb{Q}] = 3$. Since $\mathbb{Q}(x_1) \subsetneq \mathbb{Q}(x_1,x_2,x_3)$, we have that $[\mathbb{Q}(x_1,x_2,x_3) : \mathbb{Q}(x_1)] \geqslant 2$, and by the tower law we must have $[\mathbb{Q}(x_1,x_2,x_3) : \mathbb{Q}(x_1)] = 2$ as $[\mathbb{Q}(x_1,x_2,x_3) : \mathbb{Q}] \leqslant 6$. It follows that $|\mathrm{Aut}(\mathbb{Q}(x_1,x_2,x_3)|\mathbb{Q})| = 6$ and hence, by the first part of the question, $\mathrm{Aut}(\mathbb{Q}(x_1,x_2,x_3)|\mathbb{Q}) \cong S_3$.

**Aufgabe 5.** Sei $x \in \mathbb{C}$ eine Nullstelle von $X^6 + 3$. Zeige, dass $\mathbb{Q}(x)|\mathbb{Q}$ eine Galoiserweiterung ist.

*Lösungsvorschlag:*

Wegen $\operatorname{char}\mathbb{Q} = 0$ reicht es zu zeigen, daß $\mathbb{Q}(x)|\mathbb{Q}$ normal ist. Hierzu zeigen wir, daß $\mathbb{Q}(x) = L$, wobei $L \subseteq \mathbb{C}$ den Zerfällungskörper von $X^6 + 3$ über $\mathbb{Q}$ bezeichne. Es ist klar, daß $\mathbb{Q}(x) \subseteq L$. Zu zeigen ist daher nur $[\mathbb{Q}(x) : \mathbb{Q}] = [L : \mathbb{Q}]$. Da $X^6 + 3$ nach Eisenstein irreduzibel über $\mathbb{Q} = \operatorname{qf}(\mathbb{Z})$ ist, gilt $[\mathbb{Q}(x) : \mathbb{Q}] = 6$. Zu zeigen bleibt daher nur $[L : \mathbb{Q}] = 6$.

Die paarweise verschiedenen Nullstellen von $X^6 + 3$ in $\mathbb{C}$ sind offenbar $\zeta^k \mathrm{i}\sqrt[6]{3}$ $(k \in \{0, \ldots, 5\})$ mit $\zeta := e^{\frac{2\pi \mathrm{i}}{6}}$. Daher gilt $L = \mathbb{Q}(\mathrm{i}\sqrt[6]{3}, \zeta)$. Da $\mathrm{i}\sqrt[6]{3}$ genauso wie $x$ eine Nullstelle von $X^6 + 3$ ist, gilt wie oben $[\mathbb{Q}(\mathrm{i}\sqrt[6]{3}) : \mathbb{Q}] = 6$. Zu zeigen ist daher $\zeta \in \mathbb{Q}(\mathrm{i}\sqrt[6]{3})$.

Wir versuchen daher, $\zeta$ näher zu bestimmen. Offenbar bildet $\zeta$ zusammen mit den Punkten 0 und 1 ein Dreieck in der komplexen Zahlenebene, dessen vom Ursprung ausgehenden Seiten gleichlang sind (Länge 1). Dieses Dreieck hat also neben dem Innenwinkel $\frac{180^\circ}{6} = 60^\circ$ noch zwei gleichgroße Innenwinkel. Man überlegt sich leicht daß die Innenwinkelsumme in einem Dreieck $180^\circ$ beträgt, woraus folgt, daß alle Innenwinkel dieses Dreiecks $60^\circ$ betragen. Damit ist aber dieses Dreieck gleichseitig, woraus man $\zeta = \frac{1}{2} + b\mathrm{i}$ für ein $b \in \mathbb{R}$ folgt. Es folgt $\frac{1}{4} + b^2 = |\zeta| = 1$ und daher $b = \frac{\sqrt{3}}{2}$. Wegen $2b\mathrm{i} = \sqrt{3}\mathrm{i} = -(\mathrm{i}\sqrt[6]{3})^3$ folgt somit $\zeta \in \mathbb{Q}(\mathrm{i}\sqrt[6]{3})$ wie gewünscht.