Universität Konstanz Dr. Andrew Dolphin
Fachbereich Mathematik und Statistik Prof. Dr. Markus Schweighofer
Wintersemester 2010/2011

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 $a \in K \backslash \Phi_p(K)$. Zeige, dass $X^p - a \in K[X]$ irreduzibel und nicht separabel ist.

Solution

First we show irreducibility. Let $f = X^p - a$, and assume that $f = gh$, where $g,h \in K[X]$, monic and of smaller degree than f. Let L be a splitting field of f over K. Then

$$f = (X^p - a) = (X - b)^p$$

for some $b \in L$. Hence $g = (X - b)^i$ and $h = (X - b)^j$ for some $i,j \in \mathbb{N}$ such that $i + j = p$. If $i \neq 0$, since $gcd(i,p) = 1$, we can find $v,w \in \mathbb{Z}$ such that $1 = vi + wp$. Hence

$$b = b^{vi+wp} = (b^i)^v(b^p)^w = (b^i)^v a^w.$$

But $b = (b^i)^v a^w \in K$ as $b^i \in K$ (since $g \in K[X]$), which is a contradiction. Hence $i = 0$, that is f is irreducible.

To show that f is not separable, we can work over the splitting field L again. Let $\theta,\theta' \in L$ be two roots of f, then $\theta^p - \theta'^p = a - a = 0$, and hence $\theta - \theta' \in \ker(\Phi_p(L))$. But Φ_p is injective, hence $\theta = \theta'$. That is, f is inseparable.

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 $f = X^4 - 2 \in \mathbb{Q}[X]$. This is irreducible by Eisenstein. Let $\eta \in \mathbb{R}$ be the positive fourth root of 2. The f factorizes over $\mathbb{C}$ as

$$f = (X - \eta)(X + \eta)(X - \mathbb{i}\eta)(X + \mathbb{i}\eta)$$

and hence f is separable, and $\mathbb{Q}(\eta,\mathbb{i})|\mathbb{Q}$ is a Galois extension. Let $a_1 = \eta$, $a_2 = -\eta$, $a_3 = \mathbb{i}\eta$ and $a_4 = -\mathbb{i}\eta$.

We now find $[\mathbb{Q}(\mathbb{i},\eta) : Q]$. The minimum polynomial of $\mathbb{i}$ over $\mathbb{Q}(\eta)$ is X^2+1, since $\mathbb{i} \notin \mathbb{Q}(\eta) \subseteq \mathbb{R}$. So $[\mathbb{Q}(\mathbb{i},\eta) : \mathbb{Q}(\eta)] = 2$. Moreover, as f is irreducible, $[\mathbb{Q}(\eta) : \mathbb{Q}] = 4$, and hence $[\mathbb{Q}(\mathbb{i},\eta) : Q] = 8$, and hence $|\mathrm{Gal}(\mathbb{Q}(\eta,\mathbb{i})| = 8$.

Let $G = \mathrm{Gal}(\mathbb{Q}(\eta,\mathbb{i})|\mathbb{Q}) \subseteq S_4$. We have $s = (34) \in G$ (as $\overline{a_1} = a_1$, $\overline{a_2} = a_2$ and $\overline{a_3} = a_4$). One also sees that there is also a $\varphi \in G$ with $\varphi(i) = i$, and $\varphi(\eta) = \mathbb{i}\eta$, that is $r = (13)(24) \in G$. Products of these yield distinct eight $\mathbb{Q}$-automorphisms, as so

$$\{1, (1324),(12)(34), (1423),(34), (13)(24), (12), (13)(24)\} = \{1,r,r^2,r^3, s,rs,r^2s,r^3s\}.$$

We know $|G| = 8$, and hence this set is the whole Galois group. (Note one can show that $G \cong D_8$.)

The subgroups of G are as follows:

$$\begin{array}{rc}
\text{Order } 8: & G \\
\text{Order } 4: & \{1,r,r^2,r^3\} \\
 & \{1,r^2,s,r^2s\} \\
 & \{1,r^2,rs,r^3s\} \\
\text{Order } 2 & \{1,r^2\} \\
 & \{1,s\} \\
 & \{1,rs\} \\
 & \{1,r^2s\} \\
 & \{1,r^3s\} \\
\text{Order } 1 & \{1\}
\end{array}$$

There are three obvious subfields of degree 2, that is $\mathbb{Q}(\mathbb{i}), \mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\mathbb{i}\sqrt{2})$. These are the fixed fields of $\{1,r,r^2,r^3\}$, $\{1,r^2,s,r^2s\}$ and $\{1,r^2,rs,r^3s\}$ respectively.

We'll now find the fixed field of $\{1,rs\}$. Any element in $\mathbb{Q}(\eta,\mathbb{i})$ can be expressed in the form

$$x = a_0 + a_1\eta + a_2\eta^2 + a_3\eta^3 + a_4\mathbb{i} + a_5\mathbb{i}\eta + a_6\mathbb{i}\eta^2 + a_7\mathbb{i}\eta^3$$

with $a_0,\dots,a_7 \in \mathbb{Q}$. Then

$$\begin{aligned}
rs(x) &= a_0 + a_1\eta - a_2\eta^2 - a_3\eta^3 - a_4\mathbb{i} + a_5(-\mathbb{i})\mathbb{i}\eta - a_6\mathbb{i}(\mathbb{i}\eta)^2 - a_7\mathbb{i}(\mathbb{i}\eta)^3 \\
&= a_0 + a_5\eta - a_2\eta^2 - a_7\eta^3 - a_4\mathbb{i} + a_1\mathbb{i}\eta + a_6\mathbb{i}\eta^2 - a_3\mathbb{i}\eta^3.
\end{aligned}$$

Therefore x is fixed by rs if and only if

$$\begin{array}{ccc}
a_0 = a_0, & a_1 = a_5, & a_2 = -a_2, \\
a_3 = -a_7, & a_4 = -a_4, & a_5 = a_1, \\
a_6 = a_6, & a_7 = -a_3. &
\end{array}$$

Therefore a_0 and a_6 are arbitrary, $a_2 = a_4 = 0$, $a_1 = a_5$ and $a_3 = -a_7$. It follows that

$$\begin{aligned}
x &= a_0 + a_1(1+\mathbb{i})\eta + a_6\mathbb{i}\eta^2 + a_3(1-\mathbb{i})\eta^3 \\
&= a_0 + a_1((1+\mathbb{i})\eta) + \frac{a_6}{2}((1+\mathbb{i})\eta)^2 - \frac{a_3}{2}((1+\mathbb{i})\eta)^3
\end{aligned}$$

and hence the field fixed by $\{1,rs\}$ is $\mathbb{Q}((1+\mathbb{i})\eta)$.

Similarly, one can calculate that the field fixed by $\{1,r^2\}$ is $\mathbb{Q}(\mathbb{i},\sqrt{2})$, the field fixed by $\{1,s\}$ is $\mathbb{Q}(\eta)$, the field fixed by $\{1,r^2s\}$ is $\mathbb{Q}(\mathbb{i}\eta)$ and the field fixed by $\{1,r^3s\}$ is $\mathbb{Q}((1-\mathbb{i})\eta)$.

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

Solution

It is clear that $K(x^2) \subseteq K(x)$. We will show that $x \in K(x^2)$ and hence $K(x^2) \supseteq K(x)$. Assume that $x \notin K(x^2)$, then $K \subsetneq K(x^2) \subsetneq K(x)$. Since $K(x^2) \subsetneq K(x)$ we have $[K(x) : K(x^2)] > 1$, and clearly x is a root of $X^2 - x^2 \in K(x^2)[X]$, hence $[K(x) : K(x^2)] \leqslant 2$. Therefore $[K(x) : K(x^2)] = 2$. By the tower law we have that

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

but this is even, which contradicts our assumptions.

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 $[L : K] = |\mathrm{Gal}(L|K)| \leqslant 6$ and $\mathrm{Gal}(L|K) \subseteq S_3$.

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 $\mathrm{Gal}(L|K)$ has 6 elements. But $\mathrm{Gal}(L|K) \subseteq S_3$ and $|S_3| = 6$, hence $\mathrm{Gal}(L|K) = S_3$.

If $[L : K(a)] = 1$, then $[L : K] = 3$ and $\mathrm{Gal}(L|K)$ 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. Since the characteristic of $\mathbb{Q}$ is 0, the extension $L|\mathbb{Q}$ is separable. We now show that it is irreducible. If f is not irreducible, then we may write $f = f_1 f_2$ for some f_1,$f_2 \in \mathbb{Q}[X]$ with $\deg f_1 = 1$. Therefore f would have a zero $\frac{a}{b} \in \mathbb{Q}$. We can assume without loss of generality that a and b are coprime. 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 $a + b$, as a and b are coprime. But this implies that $p|b$, a contradiction. Hence $a = \pm 1$. Let q be a prime number with $p|b$. Then, since $a^2 = b^2(a + b)$ it follows that $q|a$, 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 has turning points as $\pm\sqrt{\frac{1}{3}}$, 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 $|\mathrm{Gal}(\mathbb{Q}(x_1,x_2,x_3|)|\mathbb{Q})| = 6$ and hence, by the first part of the question, $\mathrm{Gal}(\mathbb{Q}(x_1,x_2,x_3)||\mathbb{Q}) \cong S_3$.

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

Solution

We want to show that $\mathbb{Q}(x)|\mathbb{Q}$ is normal and separable. It is irreducible over $\mathbb{Q}$ (by Eisenstein). Since the characteristic of $\mathbb{Q}$ is 0 it follows that the extension is separable.

Since $X^6 + 3$ is irreducible, $[\mathbb{Q}(x) : \mathbb{Q}] = 6$.

Consider now the polynomial $f = X^3 + 3$. This polynomial is also irreducible (by Eisenstein). The splitting field for f over $\mathbb{Q}$ is $\mathbb{Q}(a,\zeta)$, where a is any root of $X^3 + 3$ and $\zeta = e^{\frac{i2\pi}{3}}$. We also have that $\mathbb{Q}(a,\zeta) : \mathbb{Q}] = 6$.

Note now that if $\mathbb{Q}(x)|\mathbb{Q}$ is normal, then X^6+3 would split in $\mathbb{Q}(x)$. In particular, $f = X^3+3$, would also split over $\mathbb{Q}(x)$ as all zeros of f are squares of zeros of X^6+3.

We want to show that $\mathbb{Q}(x) = \mathbb{Q}(a\zeta)$ (then $\mathbb{Q}(x)$ would be the splitting field of f, and hence normal). Since $[\mathbb{Q}(x) : \mathbb{Q}] = [\mathbb{Q}(a,\zeta) : \mathbb{Q}]$, it is enough to show that $\mathbb{Q}(a,\zeta) \subseteq \mathbb{Q}(x)$. We have that x^2 is a zero of f, so we may take $a = x^2$, and hence $a \in \mathbb{Q}(x)$. All that it remains to show is that $\zeta \in \mathbb{Q}(x)$.

First we show that $\zeta = \frac{1}{2} + \mathbb{i}\frac{\sqrt{3}}{2}$. This is another proof easier to follow if you draw a picture!

We know that ζ is the point on the unit circle given by the intersection in the upper half plane with a line through the origin with 60^o angle to the real axis. If we take the line from the point ζ to the intersection point of the circle with the positive part of the real axis, then we form a triangle, which with points at the origin, ζ and another point on the real line, which we call r. This forms an equilateral triangle (we know the length of 2 sides, and the angle between them. This uniquely determines the triangle), hence the real part of ζ must be $\frac{1}{2}$, as ζ is directly above the mid-point of the triangles base. The imaginary part can now be found using pythagorus.

Since $\zeta = \frac{1}{2} + \mathbb{i}\frac{\sqrt{3}}{2}$, it is clear that $\zeta \in \mathbb{Q}(x)$ if $\mathbb{i}\sqrt{3} \in \mathbb{Q}(x)$. But $(x^3)^2 = -3$, so $x^3 = \pm\mathbb{i}\sqrt{3}$, hence $\mathbb{i}\sqrt{3} \in \mathbb{Q}(x)$ and we are done.