Universität Konstanz
Fachbereich Mathematik und Statistik
Wintersemester 2010/2011

Dr. Andrew Dolphin
Prof. Dr. Markus Schweighofer

Übungsblatt 13 zur Einführung in die Algebra: Solutions

Aufgabe 1. Zeige

(a) $\mathrm{Aut}(\mathbb{Q}(\sqrt{2},\mathbb{i})|\mathbb{Q}) \cong V_4$.

(b) $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}) \cong \{1\}$.

(c) $\mathrm{Aut}(\mathbb{Q}(\sqrt[4]{2},\mathbb{i})|\mathbb{Q}(\mathbb{i})) \cong C_4$.

Solution

(a) $f = X^2+1$ and $g = X^2-2$ are the minimum polynomials of $\mathbb{i}$ and $\sqrt{2}$ over $\mathbb{Q}$ respectively and hence $\mathbb{Q}(\mathbb{i},\sqrt{2})$ is a splitting field of the polynomial $fg = (X^2+1)(X^2-2)$. By 4.3.11 any automorphism of an algebraic closure of $\mathbb{Q}$ must map $\mathbb{i}$ to either $\mathbb{i}$ or $-\mathbb{i}$ and $\sqrt{2}$ to either $\sqrt{2}$ or $-\sqrt{2}$. Hence $\mathrm{Aut}(\mathbb{Q}(\sqrt{2},\mathbb{i})|\mathbb{Q})$ has at most four elements.

$\mathbb{Q}(\mathbb{i},\sqrt{2})|\mathbb{Q}$ is a normal extension as it is the splitting field of fg. Further $\mathbb{Q}(\mathbb{i})|\mathbb{Q}$ and $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ are also normal extensions, of degree 2, by example 4.3.13. Since X^2+1 is clearly irreducible over $\mathbb{Q}(\sqrt{2})$, since for all $x \in \mathbb{R}$ we have $X^2+1 \geqslant 1$, we have $\mathbb{Q}(\mathbb{i},\sqrt{2})|\mathbb{Q}(\sqrt{2})$ is normal and of degree 2, and hence, by the tower law, $\mathbb{Q}(\mathbb{i},\sqrt{2})|\mathbb{Q}(\mathbb{i})$ is also of degree 2, and hence also normal.

Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$. Note that this will also be an algebraic closure of $\mathbb{Q}(\mathbb{i})$, $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{2},\mathbb{i})$.

Since f is a minimum polynomial over $\mathbb{Q}(\sqrt{2})$ of $\mathbb{i}$ and $-\mathbb{i}$, there exists an $\rho : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}$ such that $\rho(\mathbb{i}) = -\mathbb{i}$ and is the identity on $\mathbb{Q}(\sqrt{2})$ (by 4.3.11). By 4.3.14 (e), $\rho(\mathbb{Q}(\sqrt{2},\mathbb{i})) = \mathbb{Q}(\sqrt{2},\mathbb{i})$, and hence ρ defines an automorphism on $\mathbb{Q}(\sqrt{2},\mathbb{i})$, which (by abusing the notation) will we also call ρ. Since we know $\rho(\mathbb{i}) = -\mathbb{i}$, $\rho(\sqrt{2}) = \sqrt{2}$ and $\rho(\mathbb{Q}) = \mathbb{Q}$, we know how this automorphism acts on $\mathbb{Q}(\sqrt{2},\mathbb{i})$.

Similarly we have a element $\tau \in \mathrm{Aut}(\mathbb{Q}(\sqrt{2},\mathbb{i})|\mathbb{Q})$ such that $\tau(\sqrt{2}) = -\sqrt{2}$, $\tau(\mathbb{i}) = \mathbb{i}$ and $\tau(\mathbb{Q}) = \mathbb{Q}$.

Hence we have $\{\mathrm{id}, \rho, \tau, \tau\circ\rho\} \subseteq \mathrm{Aut}(\mathbb{Q}(\sqrt{2},\mathbb{i})|\mathbb{Q})$. But we know the automorphism has a maximum of four elements, therefore $\{\mathrm{id}, \rho, \tau, \tau\circ\rho\} = \mathrm{Aut}(\mathbb{Q}(\sqrt{2},\mathbb{i})|\mathbb{Q})$. This group is clearly isomorphic to V_4.

(b) Let $\rho \in \mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q})$ and $f = X^3-2$. Then

$$(\rho(\sqrt[3]{2}))^3 = \rho((\sqrt[3]{2})^3) = \rho(2) = 2.$$

So the $\rho(\sqrt[3]{2})$ must be another cube root of 2 for any automorphism in $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q})$. But we know (since, for example, $f'(x) \geqslant 0$ for all $x \in \mathbb{R}$) that f has only one real root, so it must have two non-real roots. But $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$, so these two roots are not elements of $\mathbb{Q}(\sqrt[3]{2})$. Hence any automorphism in $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q})$ has to map $\sqrt[3]{2}$ to itself, and since any element in $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q})$ must also be identity on $\mathbb{Q}$, we have the result.

(c) Note that over $\mathbb{C}$, the polynomial $f = X^4-2$ splits as

$$f = (X-\sqrt[4]{2})(X+\sqrt[4]{2})(X-\mathbb{i}\sqrt[4]{2})(X+\mathbb{i}\sqrt[4]{2}).$$

In particular, as in (a), this implies that there are at most four elements in $\mathrm{Aut}(\mathbb{Q}(\sqrt[4]{2},\mathtt{i})|\mathbb{Q}(\mathtt{i}))$, as every automorphism over an algebraic closure of $\mathbb{Q}(\mathtt{i})$ must map one of these roots to another.

This also shows that $\mathbb{Q}(\sqrt[4]{2},\mathtt{i})|\mathbb{Q}$ is a normal extension. The extension $\mathbb{Q}(\sqrt[4]{2})$ is of degree 4, as $\sqrt[4]{2}$ has minimum polynomial X^4-2 (which is irreducible by Eisenstein). Since we clearly have that $\mathtt{i} \notin \mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{R}$, it follows that $\mathbb{Q}(\sqrt[4]{2},\mathtt{i})|\mathbb{Q}(\sqrt[4]{2})$ is a normal extension of degree 2. We also clearly have that $\mathbb{Q}(\mathtt{i})|\mathbb{Q}$ is a normal extension of degree 2. The tower law now implies that $\mathbb{Q}(\sqrt[4]{2},\mathtt{i})|\mathbb{Q}(\mathtt{i})$ is of degree 4. Hence X^4-2 is a minimum polynomial of $\sqrt[4]{2}$ over $\mathbb{Q}(\mathtt{i})$, and hence $\mathbb{Q}(\sqrt[4]{2},\mathtt{i})$ is a splitting field for X^4-2 over $\mathbb{Q}(\mathtt{i})$, and therefore $\mathbb{Q}(\sqrt[4]{2},\mathtt{i})|\mathbb{Q}(\mathtt{i})$ is a normal extension.

Now, 4.3.11 implies that there exists an automorphism on some algebraic closure of $\mathbb{Q}(\mathtt{i})$, such that $\rho(\mathbb{Q}(\mathtt{i})) = \mathbb{Q}(\mathtt{i})$ and $\rho(\sqrt[4]{2}) = \mathtt{i}\sqrt[4]{2}$, as $\sqrt[4]{2}$ and $\mathtt{i}\sqrt[4]{2}$ have the same irreducible polynomial over $\mathbb{Q}(\mathtt{i})$. Moreover, by 4.3.14 (e) $\rho(\mathbb{Q}(\sqrt[4]{2},\mathtt{i})) = \mathbb{Q}(\sqrt[4]{2},\mathtt{i})$. Hence ρ defines an automorphism on $\mathbb{Q}(\sqrt[4]{2},\mathtt{i})$, which we will again call ρ by abuse of notation.

The map ρ acts as follows

$$\sqrt[4]{2} \mapsto \mathtt{i}\sqrt[4]{2} \mapsto -\sqrt[4]{2} \mapsto -\mathtt{i}\sqrt[4]{2}.$$

In particular $\rho^4 = \mathrm{id}$ and ρ^2 and ρ^3 are also distinct elements of $\mathrm{Aut}(\mathbb{Q}(\sqrt[4]{2},\mathtt{i})|\mathbb{Q}(\mathtt{i}))$. That is $\{\mathrm{id}, \rho, \rho^2,\rho^3\} \subseteq \mathrm{Aut}(\mathbb{Q}(\sqrt[4]{2},\mathtt{i})|\mathbb{Q}(\mathtt{i}))$. But we know the automorphism has a maximum of four elements, therefore $\{\mathrm{id}, \rho, \rho^2,\rho^3\} = \mathrm{Aut}(\mathbb{Q}(\sqrt[4]{2},\mathtt{i})|\mathbb{Q}(\mathtt{i}))$. This group is clearly isomorphic to C_4

Aufgabe 2. Sei $\alpha \in \mathbb{R}$ mit $\alpha^4 = 5$. Zeige, dass

(a) $\mathbb{Q}(\mathtt{i}\alpha^2)$ normal über $\mathbb{Q}$ ist.

(b) $\mathbb{Q}(\alpha + \mathtt{i}\alpha)$ normal über $\mathbb{Q}(\mathtt{i}\alpha^2)$ ist.

(c) $\mathbb{Q}(\alpha + \mathtt{i}\alpha)$ nicht normal über $\mathbb{Q}$ ist.

Solution

(a) We have that $(\mathtt{i}\alpha^2)^2 = -5$, so $\mathtt{i}\alpha^2$ is a root of the polynomial $X^2+5 \in \mathbb{Q}[X]$. So, $\mathbb{Q}(\mathtt{i}\alpha^2)$ is a splitting field of this polynomial (the other root is $-\mathtt{i}\alpha^2 \in \mathbb{Q}(\mathtt{i}\alpha^2)$), hence $\mathbb{Q}(\mathtt{i}\alpha^2)$ is a normal extension of $\mathbb{Q}(\mathtt{i}\alpha^2)$.

(b) We have that $(\alpha+\mathtt{i}\alpha)^2 = 2\mathtt{i}\alpha^2$, so $\alpha+\mathtt{i}\alpha$ is a root of the polynomial $X^2-2\mathtt{i}\alpha^2 \in \mathbb{Q}(\mathtt{i}\alpha^2)[X]$. So, $\mathbb{Q}(\alpha+\mathtt{i}\alpha)$ is a splitting field of this polynomial (the other root is $-\alpha-\mathtt{i}\alpha \in \mathbb{Q}(\alpha+\mathtt{i}\alpha)$), hence $\mathbb{Q}(\alpha+\mathtt{i}\alpha)$ is a normal extension of $\mathbb{Q}$.

(c) We have that $\alpha + \mathtt{i}\alpha$ is a root of the polynomial $X^4+20 \in \mathbb{Q}[X]$. This polynomial factories (over, say, $\mathbb{C}$) as

$$X^4+20 = (X-(\alpha+\mathtt{i}\alpha))(X-(-\alpha-\mathtt{i}\alpha))(X-(\alpha-\mathtt{i}\alpha))(X-(-\alpha+\mathtt{i}\alpha)).$$

So if $\mathbb{Q}(\alpha+\mathtt{i}\alpha)$ is a normal extension of $\mathbb{Q}$, then we must have that $(\alpha+\mathtt{i}\alpha)$,$(-\alpha-\mathtt{i}\alpha)$,$(\alpha-\mathtt{i}\alpha)$,$(-\alpha+\mathtt{i}\alpha) \in \mathbb{Q}$. This implies that $\mathtt{i},\alpha \in \mathbb{Q}(\alpha+\mathtt{i}\alpha)$, and hence that $\mathbb{Q}(\alpha+\mathtt{i}\alpha) = \mathbb{Q}(\mathtt{i},\alpha)$.

We know that $[\mathbb{Q}(\alpha+\mathtt{i}\alpha) : \mathbb{Q}] = 4$, and that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ (because X^4-5 is irreducible by Eisenstein), so if $\mathbb{Q}(\alpha+\mathtt{i}\alpha) = \mathbb{Q}(\mathtt{i},\alpha)$, then $\mathbb{Q}(\alpha+\mathtt{i}\alpha) = \mathbb{Q}(\alpha)$ and hence $\mathtt{i} \in \mathbb{Q}(\alpha)$. But $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$, and hence $\mathtt{i} \notin \mathbb{Q}(\alpha)$, and therefore $\mathbb{Q}(\alpha+\mathtt{i}\alpha)$ is not a normal extension of $\mathbb{Q}$.

Note, this exercise shows that normal is not a transitive property of field extension. That is, a normal extension of a normal extension is not necessarily normal.

Aufgabe 3. Sei G eine Gruppe und a,$b \in G$. Gelte $ab = ba$ und seien die Ordnungen von a und b teilerfremd (d.h. $1 \in (\mathrm{ord}\, a,\mathrm{ord}\, b)$). Zeige, dass $\mathrm{ord}\,(ab) = (\mathrm{ord}\, a)(\mathrm{ord}\, b)$.

Solution

Let $x = \operatorname{ord} a$, $y = \operatorname{ord} b$ and $z = \operatorname{ord}(ab)$. Then, since $ab = ba$, we have

$$(ab)^{xy} = a^{xy}b^{xy} = (a^x)^y(b^y)^x = 1^y 1^x = e,$$

so $z = \operatorname{ord}(ab) \leqslant (\operatorname{ord} a)(\operatorname{ord} b) = xy$.

We also have

$$(ab)^z = a^z b^z = 1,$$

so $a^z = (b^{-1})^z$, and so $((b^{-1})^z)^x = (a^z)^x = 1$, so $\operatorname{ord} b^{-1} = \operatorname{ord} b$ divides zx. But y is coprime to x, so y divides z. Similarly x divides z. Therefore $xy \leqslant z$, as x and y are coprime, and hence $xy = z$.

Aufgabe 4. Sei K ein endlicher Körper. Zeige, dass

$$K = \{b^2 + c^2 \mid b,c \in K\}.$$

Solution

Let K be a finite field having characteristic p and $|K| = p^n$. Define $\rho : K \to K$ by $\rho(x) = x^2$ for all $x \in K$.

If $p = 2$, then ρ is an isomorphism, and so for any $u \in K$ there is $v \in K$ with $u = v^2 + 0^2$.

If $p > 2$, then for all $x, y \in K$, $x^2 = y^2$ implies that $(x + y)(x - y) = 0$. Hence, $y = x$ or $y = -x$, and so $|\mathrm{Im}\ \rho| \geqslant \frac{p^n+1}{2}$ (0 is in the image, and otherwise there are at least $\frac{p^n-1}{2}$ elements in the image as $\rho(y) \neq \rho(x)$ if $x \neq y$ and $x \neq -y$. Hence there are at least $1 + \frac{p^n-1}{2} = \frac{p^n+1}{2}$ elements in the image).

Let $m = \frac{p^n+1}{2}$ and choose distinct elements $x_1^2, \dots, x_m^2 \in K$. Hence, for any $u \in K$ and for all $1 \leqslant i \leqslant m$, $u - x_i^2$ are distinct elements in K . Since $2m > p^n$, there exists j and k such that $x_j^2 = u - x_k^2$. That is, $u = x_j^2 + x_k^2$, as desired.