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

Übungsblatt 12 zur Einführung in die Algebra: Solutions

Aufgabe 1. Sei $M \subseteq \mathbb{C}$ eine Menge mit $\{0,1\} \subseteq M$. Zeige, dass für alle $z \in \mathbb{C}$ gilt

$$z \in \curlywedge M \Rightarrow \sqrt{z} \in \curlywedge M.$$

Solution

First, note that it is always possible to bisect an angle with a ruler and compass. The cases of an angle of radius 0 and π are trivial. Otherwise, draw a circle of any radius around point of the angle.Take the intersection points of the circle with the lines making up the angle you wish to bisect, and draw two circles of the same radius as above centered at these intersection point. Mark the point where they intersect within the arch of the angle A. Draw a line from the point of the angle to A. This line bisects the angle.

Suppose $w^2 = z = re^{\mathrm{i}\varphi}$. Letting $\sqrt{r}$ be the positive square root of $r \in \mathbb{R}$ we have $w = \pm\sqrt{r}e^{\mathrm{i}\varphi/2}$. Since we can bisect this angle, we only need to show that for any $r > 0$ in $\curlywedge M$, the square root $\sqrt{r}$ is also in $\curlywedge M$.

To do this we raise a perpendicular to the line between -1 and r at 0. We then draw the circle with diameter equal to the distance between -1 and r, which intersects the real line at -1 and r. The point of intersection of this perpendicular and this circle with positive imaginary part, we call v. Clearly, $|v|$ belongs to $\curlywedge M$.

The triangle with vertices -1,v and r has a right angle at v by Thales' theorem (that is, if A, B and C are points on a circle where the line between A and C is a diameter of the circle, then the angle at B is a right angle).

The formula for an altitude of a triangle now gives that $|v|^2 = 1 \cdot r$, and so $x = \sqrt{r}$.

Aufgabe 2. Sei K ein Körper und L ein Zerfällungskörper von $K[X] \setminus \{0\}$ über K. Zeige, dass L ein algebraischer Abschluss von K ist.

Solution

Clearly L is algebraic over K, so we need only show that L is algebraically closed.

Let $f \in L[X]$ be a nonconstant polynomial, and $\theta \in \overline{L}$ (some algebraic closure of L) be a root. We must show that $\theta \in L$, so denote $F = L(\theta)$. Then F/L and L/K are both algebraic extensions, so the extension F/K is also algebraic. In particular, θ is algebraic over K, so consider its minimal polynomial $g \in K[X]$. As L is the splitting field of $K[X] \setminus \{0\}$, this polynomial splits completely over L, so in particular $\theta \in L$.

Aufgabe 3. Sei K ein Körper, $f \in K[X] \setminus \{0\}$ und $n := \deg f$. Sei L der Zerfällungskörper von f über K. Zeige, dass $[L : K]$ ein Teiler von $n! = n(n-1)(n-2)\cdots 1$ ist.

Solution

We prove by induction on n that $[L : K]$ divides $n!$. Plainly, this assertion holds when $n = 1$.

Suppose then that the inductive hypothesis holds for polynomials of degree smaller than n, and consider a polynomial f of degree n. Suppose first that f is not irreducible over K, so that $f = gh$ for some polynomials $g, h \in K[X]$ of respective degrees s and t with $1 \leqslant s, t < n$ and $s + t = n$. There is a splitting field L for g over K , and by the induction hypothesis we have $[L : K] \mid s!$. We have $g = \lambda(X - \alpha_1)...(X - \alpha_s)$ for some $\lambda \in K$ and $\alpha_i \in L(1 \leqslant i \leqslant s)$. The polynomial h lies in $L[X]$. There is a splitting field M for h over L and by the induction hypothesis we have $[M : L] \mid t!$. One then has $h = \mu(X - \beta_1)...(X - \beta_t)$ for some $\mu \in K$ and $\beta_j \in L(1 \leqslant j \leqslant t)$. We now have

$$M = L(\beta_1, ..., \beta_t) = K(\alpha_1, ..., \alpha_s, \beta_1, ..., \beta_t),$$

and M is a splitting field extension for f over K. By the tower law, moreover, one has $[M : K] = [M : L][L : K]$ divides $s!t!$, which divides $(s + t)! = n!$.

When f is irreducible, there exists a simple algebraic extension $K(\alpha)$ over K, with $[K(\alpha) : K] = n$, and such that $f = (x - \alpha)h$, for some $h \in K(\alpha)[X]$ of degree $n - 1$. There exists a splitting field extension L for h over $K(\alpha)$ and by the induction hypothesis we have $[L : K(\alpha)] \mid (n - 1)!$. We may write $h = \mu(X - \beta_1)...(X - \beta_{n-1})$ for some $\mu \in K$ and $\beta_i \in L(1 \leqslant i \leqslant n - 1)$. Since $L = K(\alpha, \beta_1, ..., \beta_{n-1})$, and $f = \mu(X - \alpha)(X - \beta_1)...(X - \beta_{n-1})$, we see that L is a splitting field extension for f over K . But in this instance, the tower law yields $[L : K] = [L : K(\alpha)][K(\alpha) : K]$ divides $n(n - 1)! = n!$. The desired conclusion therefore follows by induction.

Aufgabe 4. Finde den Zerfällungskörper L von f über $\mathbb{Q}$ (genauer: beschreibe, wie er aus $\mathbb{Q}$ durch Adjunktion von wenigen möglichst „einfachen“ komplexen Zahlen entsteht) und berechne $[L : \mathbb{Q}]$, wobei

(i) $f = X^3 - 1$;

(ii) $f = X^4 + 5X^2 + 6$;

(iii) $f = X^6 - 8$.

Solution

(i) One has $f := X^3 - 1 = (X - 1)(X^2 + X + 1)$, and over $\mathbb{C}$ the polynomial $X^2 + X + 1$ splits as $(X + \omega)(X + \omega^2)$, where $\omega = \frac{1}{2}(-1 + \mathbb{i}\sqrt{3})$. Consequently, one finds that $\mathbb{Q}(\omega)$ is a splitting field extension for f over $\mathbb{Q}$. Since $X^2 + X + 1$ is irreducible over $\mathbb{Q}$, the minimal polynomial of ω over $\mathbb{Q}$ is $X^2 + X + 1$, and hence $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$.

(ii) One has $g := X^4 + 5X^2 + 6 = (X^2 + 2)(X^2 + 3)$. Let $L = \mathbb{Q}(\sqrt{-2}, \sqrt{-3})$. Then L is a splitting field extension for g over $\mathbb{Q}$, since over L one has

$$g = (X + \sqrt{-2})(X - \sqrt{-2})(X + \sqrt{-3})(X - \sqrt{-3}).$$

Furthermore, the polynomial $X^2 + 2$ is irreducible over $\mathbb{Q}$, by Eisenstein's criterion (for example). It follows that $\sqrt{-2}$ has minimal polynomial $X^2 + 2$ over $\mathbb{Q}$, and hence $[\mathbb{Q}(\sqrt{-2}) : \mathbb{Q}] = 2$. The polynomial $X^2 + 3$ is irreducible over $\mathbb{Q}(\sqrt{-2})$, for if $\sqrt{-3} = a + b\sqrt{-2}$ for some $a, b \in \mathbb{Q}$, then $-3 = (a + b\sqrt{-2})^2 = (a^2 - 2b^2) + 2ab\sqrt{-2}$, so that $2ab = 0$. Then $a = 0$, in which case $-3 = -2b^2$, or else $b = 0$, in which case $a^2 = -3$. Neither of these equations are soluble in $\mathbb{Q}$, and so we must conclude that $X^2 + 3$ is the minimal polynomial of $\sqrt{-3}$ over $\mathbb{Q}(\sqrt{-2})$, whence $[\mathbb{Q}(\sqrt{-3}, \sqrt{-2}) : \mathbb{Q}(\sqrt{-2})] = 2$. We now deduce from the tower law that

$$[L : \mathbb{Q}] = [\mathbb{Q}(\sqrt{-3}, \sqrt{-2}) : \mathbb{Q}(\sqrt{-2})][\mathbb{Q}(\sqrt{-2}) : \mathbb{Q}] = 2^2 = 4.$$

(iii) One root of $h := X^6 - 8$ over $\mathbb{C}$ is $8^{\frac{1}{6}} = \sqrt{2}$. Dividing through by $(\sqrt{2})^6$ and writing T for $X/\sqrt{2}$, we obtain the polynomial $T^6 - 1$. Write ω for a primitive sixth root of unity, say $e^{2\pi\mathbb{i}/6} = \frac{1}{2}(1 + \mathbb{i}\sqrt{3})$. Then

$$T^6 - 1 = (T - 1)(T - \omega)(T - \omega^2)(T - \omega^3)(T - \omega^4)(T - \omega^5),$$

and hence

$$h = (X - \sqrt{2})(X - \omega\sqrt{2})(X - \omega^2\sqrt{2})(X - \omega^3\sqrt{2}))(X - \omega^4\sqrt{2})(X - \omega^4\sqrt{2}).$$

Thus $\mathbb{Q}(\sqrt{2}, \sqrt{-3})$ is a splitting field extension for h over $\mathbb{Q}$, and an argument similar to that of part (ii), save with $\sqrt{2}$ in place of $\sqrt{-2}$, shows that $[\mathbb{Q}(\sqrt{2}, \sqrt{-3}) : \mathbb{Q}] = 4$. In fact the argument is simpler in this case, as it is clear that $\mathbb{Q}(\sqrt{-3}) \nsubseteq \mathbb{Q}(\sqrt{2})$ as $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$.