Universität Konstanz
Fachbereich Mathematik und Statistik
Wintersemester 2010/2011

Dr. Andrew Dolphin
Prof. Dr. Markus Schweighofer

Übungsblatt 11 zur Einführung in die Algebra: Solutions

Aufgabe 1. Für jede Teilmenge M der komplexen Zahlenebene $\mathbb{C} = \mathbb{R} \oplus \mathbb{R}\mathbb{i} \cong \mathbb{R}^2$ sei

$$\begin{aligned} \mathrm{Ge}(M) &= \text{Menge der Geraden, die zwei verschiedene Punkte von } M \text{ enthalten} \\ \mathrm{Kr}(M) &= \text{Menge der Kreise, deren Mittelpunkt in } M \text{ liegt und deren} \\ &\quad\ \text{Radius gleich dem Abstand zweier Punkte aus } M \text{ ist.} \end{aligned}$$

Wir betrachten dann die folgenden *elementaren Konstruktionsschritte*:

($\times$) Schnitt zweier verschiedener Geraden aus $\mathrm{Ge}(M)$

($\varnothing$) Schnitt einer Geraden aus $\mathrm{Ge}(M)$ mit einem Kreis aus $\mathrm{Kr}(M)$

($\circledcirc$) Schnitt zweier verschiedener Kreise aus $\mathrm{Kr}(M)$.

Für jede Menge $M \subseteq \mathbb{C}$ sei $M' \subseteq \mathbb{C}$ die Menge M vereinigt mit den Schnittpunkten, die man durch Anwendung von ($\times$), ($\varnothing$) und ($\circledcirc$) erhalten kann. Man nennt die Elemente von M' die in einem Schritt aus M konstruierbaren Punkte. Nun definieren wir für $M \subseteq \mathbb{C}$ induktiv die Menge $M^{(n)}$ der in n Schritten ($n \in \mathbb{N}_0$) aus M konstruierbaren Punkte durch $M^{(0)} := M$ und $M^{(n+1)} := (M^{(n)})'$ für $n \in \mathbb{N}_0$. Schließlich sagen wir, die Punkte aus

$$\measuredangle M := \bigcup \{M^{(n)} \mid n \in \mathbb{N}\}$$

sind *mit Zirkel und Lineal aus M konstruierbar*. Zeige durch geometrische Konstruktionen (stichpunktartig kommentierte Skizzen), dass für jedes $M \subseteq \mathbb{C}$ mit $\{0,1\} \subseteq M$, die Menge $\measuredangle M$ einen Zwischenkörper von $\mathbb{C}|\mathbb{Q}(\mathbb{i})$ bildet.

Solution

The reasoning in these solutions is easier to follow if you draw a picture to go along with it! We'll show the following results, which together show that $\measuredangle M$ is a field that contains $\mathbb{Q}(\mathbb{i})$.

(1) $\mathbb{i} \in \measuredangle M$

(2) $z \in \measuredangle M \Rightarrow \overline{z} \in \measuredangle M$

(3) $z \in \measuredangle M \Rightarrow \mathrm{R}e(z), \mathrm{I}m(z) \in \measuredangle M$

(4) $z \in \measuredangle M \Rightarrow -z \in \measuredangle M$

(5) $z_1, z_2 \in \measuredangle M \Rightarrow z_1 + z_2 \in \measuredangle M$

(6) $z_1, z_2 \in \measuredangle M \Rightarrow z_1 z_2 \in \measuredangle M$

(7) $z \in \measuredangle M, z \neq 0 \Rightarrow \frac{1}{z} \in \measuredangle M$.

(Note that (3) is not needed to prove our final result, but will be needed in order to prove some of the other statements)

(1) The line connecting 0 and 1, that is, the real line $\mathbb{R}$, belongs to $\mathrm{Ge}(M)$ by definition. Intersecting $\mathbb{R}$ with the unit circle, which belongs to $\mathrm{Kr}(M)$, we see that $-1 \in \curlywedge M$. We can then construct the perpendicular bisector of the interval $[1:1]$. That is, we construct a line passing through the intersection points of two circles, centered at 1 and -1, of radius 2. We then intersect this line with the unit circle, and we obtain $\mathbb{i} \in \curlywedge M$.

(2) Drop a perpendicular from z to $\mathbb{R}$. This is done by drawing a circle around z of diameter large enough so that it crosses $\mathbb{R}$ at two points. The perpendicular from z to $\mathbb{R}$ is then found by constructing the perpendicular bisector of this point. From the foot of this perpendicular, say a, draw a circle whose radius is the distance from a to z . Its second intersection with the straight line through z and a gives $\overline{z} \in \curlywedge M$

(3) As just verified, we have $a = \mathrm{R}e(z) \in \curlywedge M$. To obtain $a = \mathrm{I}m(z) \in \curlywedge M$, draw the perpendicular to the imaginary axis through z , and then transfer to $\mathbb{R}$ the absolute value of the foot b of the perpendicular.

(4) Intersect the line through 0 and z with the circle of radius $|z|$ and center 0.

(5) In the case where $z_1 \neq z_2$, intersect the circle of center z_1 and radius $|z_2|$ with the circle of center z_2 and radius $|z_1|$. One of the intersections is the vertex $z_1 + z_2$ of the parallelogram determined by z_1, z_2.

In the case $z_1 = z_2$, intersect the line between 0 and z_1 with the circle centre z_1, radius the length of the line between 0 and z_1. The intersection point not at 0 is $z_1 + z_1$.

(6) If $z_1 = a + \mathbb{i}b_1$ and $z_2 = a_2 + \mathbb{i}b_2$ we have

$$z_1 z_2 = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1)i.$$

Now $z_1, z_2 \in \curlywedge M$ implies that $a_1, a_2, b_1, b_2 \in \curlywedge M$ by (3). So if this claim is true for real numbers, then it will also be true for arbitrary complex numbers by (4) and (5). Therefore we must prove that given real numbers r_1 and r_2,

$$r_1, r_2 \in \curlywedge M \Rightarrow r_1 r_2 \in \curlywedge M.$$

We may assume that $r_1, r_2 > 0$. Consider intersection point of the line through 0 and $1 + \mathbb{i}$ with the circle of radius r_2 and centre 0 with positive real part, which we call z. We then construct the line through z and 1.

We now construct a line parallel to the line through z and 1 going through r_1. We do this by dropping a perpendicular from r_1 to the line, then constructing a perpendicular to this second line through r_1.

This line crosses the line between 0 and z at y.

Now we have constructed 2 similar triangles, one with vertices at 0, 1 and z with the length of the line between 0 and z being r_2, and one with vertices at 0, r_1 and y with the length of the line between 0 and y being x. These triangles are similar, hence the ratio of x to r_1 is equal to the ratio of r_2 to 1. That is, $x = r_1 r_2$. Hence $r_1 r_2 \in \curlywedge M$

(7) Since $z^{-1} = \overline{z} \cdot (z\overline{z})^{-1}$, it suffices in view of the earlier parts to show that if $r > 0$ lies in $\curlywedge M$, so does r^{-1}. We again construct a part of similar triangles.

For the first triangle, we draw a circle of radius 1, and take the intersect point of this circle with the line through 0 and $1 + \mathbb{i}$ whose real part is positive, to give the first vertex, x. We then form a triangle with vertices at 0, r and x with the length of the line between 0 and x being 1.

For the second triangle, we construct a parallel line through 1 to the line between x and r. This intersects the line between 0 and $1 + i$ at the point y. We then form the triangle with vertices at 0, 1 and y. This triangle is similar to the previously drawn triangle, and hence the ratio of r to 1 is equal to the ratio of 1 to the length of the line between 0 and y. Hence the length of the line between 0 and y is $1/r$.

We can hence construct r^{-1} by the intersection of $\mathbb{R}$ and the circle, centre 0, radius the length of the line between 0 and y.

Aufgabe 2. Sei $L|K$ eine Körpererweiterung und $a,b \in L$ mit $a^2 \in K$ und $b^2 \in K$.

(a) Finde ein Polynom $f \in K[X] \setminus \{0\}$ mit $f(a+b) = 0$.

(b) Welche Grade kommen für das Minimalpolynom $\mathrm{irr}_K(a+b)$ von $a+b$ über K in Frage? Gebe jeweils ein Beispiel für jeden möglichen Grad und ein stichhaltiges Argument für jeden unmöglichen Grad.

Solution

(a) Since
$$(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4$$
and
$$(a^2+b^2)(a+b)^2 = a^4 + 2a^3b + 2a^2b^2 + 2ab^3 + b^4$$
we have that $a+b$ is a root of the polynomial
$$X^4 - 2(a^2+b^2)X^2 - 2a^2b^2 + a^4 + b^4$$
whose coefficients are in K.

(b) Higher degrees than 4 are clearly not possible, as $a+b$ is always a root of the polynomial $X^4 - 2(a+b)X^2 - 2ab + a^2 + b^2$ over K. Moreover, let $F := K(a,b) \supseteq K(a+b)$. $[F:K] = [F:K(a)][K(a):K]$, and hence is either $1, 2$ or 4. We must have that $[K(a+b):K]$ divides $[F:K]$. Hence $[K(a+b):K] \neq 3$.

Degree one is possible. Take $a,b \in K$, then $K(a) = K$ and the minimal polynomial of $a+b$ is $X - a - b$. For example, $K = \mathbb{R}$ and $a = 4$, $b = 4$.

Degree two is possible. For example, let $K = \mathbb{Q}, a = \sqrt{2}, b = 1$. Then the minimal polynomial of $a+b$ over K is $X^2 - 2X - 1$.

Degree four is possible. We shall see in the next question that $X^4 - 16X^2 + 4$ is the minimal polynomial of $\sqrt{3} + \sqrt{5}$ over $\mathbb{Q}$

Aufgabe 3. Bestimme die Minimalpolynome von $\sqrt{3} + \sqrt{5}$ über $\mathbb{Q}, \mathbb{Q}(\sqrt{5})$ und $\mathbb{Q}(\sqrt{15})$.

Solution

Consider the tower $\mathbb{Q} \subset \mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\sqrt{5}, \sqrt{3})$. As $\sqrt{5} \notin \mathbb{Q}$, $x^2 - 5$ is the minimal polynomial of $\sqrt{5}$ over $\mathbb{Q}$ and we have that $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2$. Furthermore, $\sqrt{3} \notin \mathbb{Q}(\sqrt{5})$, as we now show.

Since the equation $3 = (a + b\sqrt{5})^2 = a^2 + 5b^2 - 2ab\sqrt{5}$ implies that a or b must be 0. If $b = 0$, this 3 implies that 3 is a square in $\mathbb{Q}$, which is false. If $a = 0$, this implies that $3/5$ is a square in $\mathbb{Q}$. Assume $3/5 = p^2/q^2$, where p and q are coprime. Then $3q^2 = 5p^2$, which is clearly impossible.

It follows, using the product formula, that $[\mathbb{Q}(\sqrt{5}, \sqrt{3}) : \mathbb{Q}] = 4$.

Consider the tower $\mathbb{Q} \subset \mathbb{Q}(\sqrt{15}) \subset \mathbb{Q}(\sqrt{3} + \sqrt{5}) \subset \mathbb{Q}(\sqrt{3}, \sqrt{5})$, where the second inclusion follows from $(\sqrt{3} + \sqrt{5})^2 = 8 + 2\sqrt{15}$.

The first inclusion is proper as $\sqrt{15} \notin \mathbb{Q}$ and so is the second, as we now show. If $\mathbb{Q}(\sqrt{15}) = \mathbb{Q}(\sqrt{3} + \sqrt{5})$, then $\sqrt{3} + \sqrt{5}$ would be an element of $\mathbb{Q}(\sqrt{15})$ and hence so is
$$\sqrt{15}(\sqrt{3} + \sqrt{5}) = 3\sqrt{5} + 5\sqrt{3}$$

and hence

$$\frac{1}{2}(3\sqrt{5}+5\sqrt{3}-3(\sqrt{3}+\sqrt{5})) = \sqrt{3} \in \mathbb{Q}(\sqrt{15}).$$

Since $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{15}) : \mathbb{Q}]$, this implies that $\mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\sqrt{15})$. Similarly, one can argue that we would also get $\mathbb{Q}(\sqrt{4}) = \mathbb{Q}(\sqrt{15})$. But $\mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\sqrt{5})$, as we argued above, hence the inclusion is proper.

It follows, by considering the possible degrees, that $\mathbb{Q}(\sqrt{3}+\sqrt{5}) = \mathbb{Q}(\sqrt{3},\sqrt{5})$.

Note that $\mathbb{Q}(\sqrt{5})(\sqrt{3}+\sqrt{5}) = \mathbb{Q}(\sqrt{3},\sqrt{5})$ and $\mathbb{Q}(\sqrt{15})(\sqrt{3}+\sqrt{5}) = \mathbb{Q}(\sqrt{3},\sqrt{5})$. Hence, the minimal polynomial of $\sqrt{3}+\sqrt{5}$ is of degree 4 over $\mathbb{Q}$ and of degree 2 over $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{15})$.

Finally, using 2 (a), we obtain that $X^4 - 16X^2 + 4$ is the minimal polynomial of $\sqrt{3}+\sqrt{5}$ over $\mathbb{Q}$, $X^2 - 2\sqrt{5}X + 2$ is the minimal polynomial over $\mathbb{Q}(\sqrt{5})$ and $X^2 - 8 - 2\sqrt{15}$ over $\mathbb{Q}(\sqrt{15})$.

Aufgabe 4. Sei $L|K$ eine Körpererweiterung mit $2 \neq 0$ in K und gelte $[L : K] = 2$.

(a) Zeige, dass es ein $x \in L$ gibt mit $L = K(x)$ und $x^2 \in K$.

(b) Zeige $\{b^2 \mid b \in L\} \cap K = \{a^2 \mid a \in K\} \cup \{(ax)^2 \mid a \in K\}$ für jedes x wie in (a).

Solution

(a) Let $\alpha \in L \setminus K$, then $L = K(\alpha)$. If $X^2 + bX + c \in K[X]$, for $b,c \in K$ is the minimal polynomial of α over K. By completing the square, we can rewrite this minimal polynomial as $(X - \frac{b}{2})^2 - \frac{b^2}{2} + c$. Let $x = (\alpha + \frac{b}{2}) \in L$. Then $K(\alpha) = K(x)$ and $x^2 = \frac{b^2}{4} - c \in K$

(b) Note that $1, x$ is a basis for L as a K–vector space. Let $\alpha \in K^\times$ be a square in L, then $\alpha = (u+vx)^2 = u^2 + x^2v^2 + 2uvx$ for some $u,v \in K$. Since $2 \neq 0$ in K, it follows that $uv = 0$. If $u = 0$ then $\alpha \in \{(ax)^2 \mid a \in K\}$, if $v = 0$ then $\alpha \in \{a^2 \mid a \in K\}$.