D-MATH Algebra II FS 2014
Prof. Brent Doran

Solutions 5

1. Show that $\sqrt{7}$, $e^{2\pi i/17}$, $\sqrt{2}+\sqrt[3]{5}$ are algebraic integers over $\mathbb{Q}$. Show that all complex numbers are algebraic over $\mathbb{R}$.

   Solution : We have $(\sqrt{7})^2 - 7 = 0$, $(e^{2\pi i/17})^{17} - 1 = 0$. Set $\alpha = \sqrt{2} + \sqrt[3]{5}$. Then $(\alpha - \sqrt{2})^3 = 5$ and
   $$\alpha^3 + 6\alpha - 5 = \sqrt{2}(2 + 3\alpha^2)$$
   so that
   $$(\alpha^3 + 6\alpha - 5)^2 - 2(2 + 3\alpha^2)^2 = 0.$$
   Finally, for $z = x + iy \in \mathbb{C}$, $(z - x)^2 + y^2 = 0$.

2. Let d, d' be square-free integers.

   (a) Show that $\mathrm{Aut}(\mathbb{Q}[\sqrt{d}])$ is a group of order two, that consists of the identity and the map $\sigma(a + b\sqrt{d}) = a - b\sqrt{d}$.

   Solution : We know that $\mathbb{Q}[\sqrt{d}])$ has basis $(1, \sqrt{d})$. If we take f to be an automorphism of $\mathbb{Q}[\sqrt{d}]$, it needs to preserve 1. Hence $f(n) = n$ for every integer n, and
   $$f(\sqrt{d})^2 = f(d) = d$$
   implies that $f(\sqrt{d})$ is either $+\sqrt{d}$ or $-\sqrt{d}$.

   (b) When are $\mathbb{Q}[\sqrt{d}]$ and $\mathbb{Q}[\sqrt{d'}]$ not isomorphic ? Conclude that there are countably many distinct quadratic number fields $\mathbb{Q}[\sqrt{d}]$.

   Solution : Assume that $\sqrt{d'} \in \mathbb{Q}[\sqrt{d}]$. This means that there exists an element $x = a + b\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$ such that $x^2 = d'$. More precisely,
   $$a^2 + b^2 d + 2ab\sqrt{d} = d',$$
   so that either a or b needs to be 0. If $b = 0$, this would mean that $d' = a^2$ is the square of an integer and this can not happen by assumption. So $a = 0$ and $d'/d = b^2$. In fact, there exists x as above if and only if $d'/d = b^2$. It follows that if we take $d' = p$, $d = q$ prime numbers, the quadratic number fields they define are not isomorphic, since primes can not be squares. We conclude with the fact that there are countably many primes.

(c) Show that uncountably many transcendental numbers exist.

Solution : By definition, the set of all algebraic numbers is a subset of

$$\bigcup_{f(x)\in Q[x]} \{\alpha \in \mathbb{C} : f(\alpha) = 0\} = \bigcup_{n\geqslant 0} \bigcup_{\substack{f(x)\in\mathbb{Q}[x] \\ deg f(x)=n}} \{\alpha \in \mathbb{C} : f(\alpha) = 0\},$$

i.e. countable unions over countable sets (the second union is taken over a subset of $\mathbb{Q}^{n+1}$) of finite sets. Hence there are countably many algebraic numbers, and since the complex numbers are uncountable, there must be uncountably many transcendental numbers.

3. Determine the integer d for which the polynomials

$$f(x) = x^5 - 8x^3 + 9x - 3, \qquad g(x) = x^4 - 5x^2 - 6x + 3$$

have a common root in $\mathbb{Q}[\sqrt{d}]$.

Solution : Consider the ideal $\mathfrak{I} = (f(x), g(x))$. Since $\mathbb{Q}[x]$ is a principal ideal domain, $\mathfrak{I}$ is generated by a single polynomial $h(x)$. Note that α is a root of h if and only if it is a common root of $f(x)$ and $g(x)$. By the Euclidean algorithm, we establish that

$$h(x) = x^2 - 3x + 1.$$

Hence f and g have exactly two common roots

$$\frac{3}{2} \pm \frac{1}{2}\sqrt{5}.$$

4. For which negative integers $d \equiv 2 \bmod 4$ is the ring if integers in $\mathbb{Q}[\sqrt{d}]$ a unique factorisation domain ?

Solution : Let $K = \mathbb{Q}[\sqrt{d}]$ for $d < 0$ such that $d \equiv 2 \bmod 4$ and let $\mathcal{O}_K$ denote the ring of integers in K. We know that $\mathcal{O}_K$ is the ring of all elements of the form $a + b\sqrt{d}$ with $a, b \in \mathbb{Z}$. We also know that the units of $\mathcal{O}_K$ are ± 1 and that factoring terminates in $\mathcal{O}_K$. If $d \equiv 2 \bmod 4$ and is negative, then $4 - d$ is an even, positive integer, and factors in two ways in $\mathcal{O}_K$:

$$4 - d = 2\left(\frac{4-d}{2}\right) = \left(2 - \sqrt{d}\right)\left(2 + \sqrt{d}\right).$$

For $\mathcal{O}_K$ to be a unique factorisation domain, we would need 2, as a prime, to divide either $2 - \sqrt{d}$ or $2 + \sqrt{d}$ in $\mathcal{O}_K$. We can check using the size function that 2 is irreducible for $d < -2$. For $d = -2$, the ring $\mathcal{O}_K$ is a Euclidean domain. The proof of this is similar to Exercise 1, problem set 3. Hence, for $d \equiv 2 \bmod 4$ negative, $\mathbb{Q}[\sqrt{d}]$ is a unique factorization domain only for $d = -2$.