Prof. Dr. Marcus Greferath
Dept. of Mathematics and Systems Analysis
School of Sciences
Aalto University

Spring 2019

MS-E1997: Abstract Algebra II

Problem Set IV

Problem 1: Show: If $G : F$ is a field extension of prime degree, then $G = F(a)$ for each $a \in G \setminus F$.

Work: It is clear that $F(a)$ is an intermediate field of the extension $G : F$, and hence $p = [G : F] = [G : F(a)] \cdot [F(a) : F]$. As $F(a) \neq F$ for $a \notin F$ we have $[F(a) : F] = p$ and this implies $G = F(a)$.

Problem 2: Assume $F(a) : F$ is a field extension where a is transcendental over F.

(a) Show that every element in $F(a) \setminus F$ is transcendental over F.

(b) $F(a) = \{f(a)g(a)^{-1} \mid f, g \in F[x], g \neq 0\}$, meaning that $F(a)$ is isomorphic to the field of rational functions over F.

Work: **(a)** As we will learn below in **(b)** every element of $F(a)$ is of the form $f(a)/g(a)$ for some $f, g \in F[x]$ with $g \neq 0$, where we may assume that $\gcd(f, g) = 1$. If such an element is in F then clearly f and g are constant, so assume this is not the case and that $f(a)/g(a)$ is not transcendental. Then there exists a (non-constant) polynomial $h \in F[x]$ of minimal degree n such that $h(f(a)/g(a)) = 0$. To see what this really means, write $h = \sum_{i=0}^{n} h_i x^i$ and then we have

$$h(f(a)/g(a)) \;=\; \sum_{i=0}^{n} h_i f^i(a)/g^i(a) \;=\; 0.$$

Multiplying this by $g^n(a)$ we find that $\sum_{i=0}^{n} h_i f^i(a) g^{n-i}(a) \;=\; 0$, and thus we have found the polynomial $\sum_{i=0}^{n} h_i f^i g^{n-i} \in F[x]$ that has a as zero. As a is transcendental we know $0 = \sum_{i=0}^{n} h_i f^i g^{n-i}$ or better $h_n f^n = -\sum_{i=0}^{n-1} h_i f^i g^{n-i}$ But then every irreducible factor of g also divides f, a contradiction to f and g being coprime.

(b) First of all we observe that the set $T := \{f(a)g(a)^{-1} \mid f, g \in F[x], g \neq 0\}$ forms a field extension of F that contains a. In fact by the transcendence of a we have $g(a) \neq 0$ for all $g \neq 0$, and the remaining field axioms are easy to verify. Hence $F(a) \subseteq T$. On the other hand every field extension of F that contains a must contain all expressions of the form $f(a)/g(a)$ with $f, g \in F[x]$ and $g \neq 0$, and hence it must contain T. For this reason we have $F(a) \supseteq T$ which finally yields $F(a) = T$. For the isomorphism just use the substitution $x \mapsto a$.

Problem 3: For every $n \in \mathbb{N}$ let $a_n \in \mathbb{C}$ be a zero of the rational polynomial $x^n - 2$, and let $L := \mathbb{Q}(\{a_n \mid n \in \mathbb{N}\})$. Now show the following:

(a) $L : \mathbb{Q}$ is an algebraic field extension.

(b) $[L : \mathbb{Q}] = \infty$.

Work: **(a)** Observe first that

$$L = \bigcup_{n \in \mathbb{N}} \mathbb{Q}(\{a_i \mid i \leq n\}).$$

For this reason every $z \in L$ is contained in some $\mathbb{Q}(\{a_i \mid i \leq n\})$ for suitable $n \in \mathbb{N}$. The latter extension is finite and hence algebraic over $\mathbb{Q}$ and thus we have recognized the extension that we started with to be algebraic.

(b) For the infinity of degree we have $\mathbb{Q}(\{a_n\})$ being an intermediate field of $L : \mathbb{Q}$, and hence $[L : \mathbb{Q}] \geq [\mathbb{Q}(a_n) : \mathbb{Q}] = n$ for all $n \in \mathbb{N}$, accepting that $x^n - 2$ is irreducible over $\mathbb{Q}$ by Eisensteins criterion.

Problem 4: In the Euclidean plane there is given a line segment of length 1 and the parabola T described by the equation $y = x^2$. Assume that we allow for the usual compass and straightedge constructions, and in addition we allow for intersections of constructible sets with T.

(a) Determine those integers $m \in \mathbb{N}$ for which $\sqrt[m]{2}$ can be constructed.

(b) Describe a construction of the number $\sqrt[3]{2}$.

Work: Using just compass and straightedge we will not get beyond the results that we had in class. But certainly we can construct $\sqrt[m]{2}$ for all m which are a power of 2. Using the parabola $y = x^2$ and intersecting it with the circle defined by $(x-a)^2 + (y-b)^2 = c^2$ we end up with the equation $x^4 + (1-2b)x^2 - 2xa = c^2 - a^2 - b^2$. Choosing $c^2 = a^2 + b^2$ makes this circle pass the origin. Then choosing $b = 1/2$ we find that the square expression vanishes, so that we end up with the equation $x^4 - 2xa = 0$. As the origin intersection is not the important one, we obtain $x^3 = 2a$ from this. For $a = 1$ we thus have constructed the number $\sqrt[3]{2}$, hence yielding a solution of **(b)**. If $z := \sqrt[3^n]{2}$ has already been constructed, then we set $a := z/2$ and come up with a construction of $\sqrt[3^{n+1}]{2}$. This shows by induction and our earlier results that we are able to construct $\sqrt[m]{2}$ for all $m = 2^n 3^k$ where $n, k \in \mathbb{N}$. This solves the question under **(a)**.

Additional Remark: Why is it exactly these values? To answer this let us inspect our proceeding in the lecture: Corollary 2.52 is certainly still true, as is Lemme 2.53. Extending this lemma we need to analyze line-parabola intersections and circle-parabola intersections. Intersecting a line of the form $y = ax + b$ with the parabola $y = x^2$ algebraically does not imply more than the solution of a quadratic equation, and we know already that this does not involve anything else than drawing square roots. As seen above, intersecting the parabola with an arbitrary circle involves solving an equation of degree at most 4 on the algebraic side. It is known (see for example `www.mathworld.wolfram.com`) that this can be done by drawing square and cubic roots. This induces an immediate modification of Theorem 2.54, where the square root expressions simply need to be exchanged by square or

cubic root expressions. Corollary 2.55 then states that a constructible element necessarily lies in a field extension H of $\mathbb{Q}$ with $[H : \mathbb{Q}] = 2^n 3^m$ for suitable $n, m \in \mathbb{N}$. Then it follows that for every prime $p \geq 5$ we cannot construct $\sqrt[p]{2}$, and hence, exactly the k-th roots of 2 (or any other constructible number) can be drawn where k is of the form $2^n 3^m$.

You are encouraged to collaborate in preparing solutions, however, please submit individual write-ups.