NAP 2019, MODULE II, HOMEWORK ASSIGNMENT #2

Michel Waldschmidt

Homework assignment, June 3, 2019.

- Problem 5.3 p. 50.

  Let K be a finite field, q the number of elements in K. Given a polynomial f of degree d in $K[x]$, we list the polynomials g of degree $\leq d/2$ with coefficients in K. The set of these polynomials is finite (with at most $q^{(d/2)+1}$ elements). For each of them we divide f by g (using the Euclidean division) and we check whether the remainder is 0 or not. If one remainder is 0, then this g divides f. Otherwise f is irreducible in $K[x]$.

- Problem 5.4 p. 50.

  As suggested in the assignment, we first check that $f - yg$ is irreducible as a polynomial in x with coefficients in the ring $K[y]$, where x and y are independent variables and f, g are in $K[x]$ without common factor.

  Indeed, if $f - yg$ factors as hk with h and k in $K[y][x] = K[x, y]$, then the degree in y of one of the two polynomials h, k is 1 and the degree of the other is 0; therefore one of the two factors is in $K[x]$ and divides both f and g. Since f and g are relatively prime in $K[x]$, we deduce that this factor is a constant. Hence $f - yg$ is irreducible.

  We now use Gauss's Lemma (Corollary of Theorem 3.12). The quotient field of the ring $R = K[y]$ is $F = K(y)$. Since $f - yg$ is irreducible over the ring $R = K[y]$, it is also irreducible over the ring $F[x] = K(y)[x]$.

- Problem 5.5 p. 51.

  Compare with Problems 4.8 p. 47 and 4.10 p. 48.

  Since $\beta \in K(\alpha)$, there exist polynomials P and Q with $Q \neq 0$ such that $\beta = P(\alpha)/Q(\alpha)$. There is such a pair of polynomials that are relatively prime in $K[x]$. Let $d = \max\{\deg P, \deg Q\}$. Since $\beta \notin K$, the rational fraction P/Q is not constant and $d \geq 1$. The polynomial $P(x) - \beta Q(x) \in \mathbb{Q}(\beta)[x]$ has degree d and vanishes at α, hence α is algebraic of degree $\leq d$ over $K(\beta)$ and therefore $K(\alpha) : K(\beta)$ is a finite extension of degree $\leq d$. Since $K(\alpha)$ has infinite degree over K, it follows that $K(\beta)$ has also infinite degree over K, which means that β is transcendental over K.

  From Problem 5.4 p. 50. we deduce that the polynomial $P(x) - \beta Q(x)$ is irreducible over the field $K(\beta)$ (recall that, β being transcendental over K, the field $K(\beta)$ is isomorphic to the field of rational fractions $K(y)$). Hence $P(x) - \beta Q(x)$ is the minimal polynomial of α over $K(\beta)$ and therefore $[K(\alpha) : K(\beta)] = d$.

- Problem 5.6 p. 51–52.

  The polynomial

  $$f(x) = a_0 + a_1 x + \cdots + a_{d-1} x^{d-1} + a_d x^d$$

  is irreducible if and only if the polynomial

  $$x^d f(1/x) = a_0 x^d + a_1 x^{d-1} + \cdots + a_{d-1} x + a_d$$

  is irreducible.

- Problem 5.7 p. 52.

  Use Eisenstein criterion with $R = \mathbb{Z}$, $f = x^n - p$. The coefficients are relatively prime, p divides all coefficients apart from the leading one $f_n = 1$, and p^2 does not divide the constant coefficient $f_0 = -p$.

- Problem 5.8 p. 52.

For each $n \geq 1$ the field A of real algebraic numbers contains $\sqrt[n]{2}$ which has degree n over $\mathbb{Q}$ (Problem 5.7), hence the degree of A over $\mathbb{Q}$ is $\geq n$. Therefore $[A : \mathbb{Q}] = \infty$.

- Problem 5.9 p. 52.

Let E and F be two subfields of a field L which are finite extensions of K of relatively prime degrees m and n. The degree of the field $K(E, F)$ over K is $\leq mn$ (Problem 4.2 p. 45). Since $K(E, F)$ contains E and F, this degree is a multiple of m and n, hence it is mn.

Now by induction we deduce from Problem 5.7 that the degree over $\mathbb{Q}$ of the field

$$\mathbb{Q}(\sqrt[2]{2}, \sqrt[3]{2}, \sqrt[5]{2}, \dots, \sqrt[p]{2})$$

is the product of the prime numbers $2 \cdot 3 \cdot 5 \cdots p$.

If we had a linear relation

$$a_2\sqrt{2} + a_3\sqrt[3]{2} + a_5\sqrt[5]{2} + \cdots + a_p\sqrt[p]{2} = 0$$

with $a_2, a_3, \dots, a_p$ in $\mathbb{Q}$ and $a_p \neq 0$, it would imply that the degree of $\sqrt[p]{2}$ over $\mathbb{Q}$ is not a multiple of p, a contradiction with Problem 5.7.

- Problem 5.10 p. 52.

We could extend Eisenstein Criterion to $\mathbb{Z}[i]$ but we can also prove the results as follows.

The two polynomials $x^5 - 4x + 2$ and $x^4 - 4x + 2$ are irreducible over $\mathbb{Q}$ by Eisenstein criterion with $p = 2$.

Let α be a root in $\mathbb{C}$ of $x^5 - 4x + 2$. The degree over $\mathbb{Q}$ of $\mathbb{Q}(\alpha)$ is 5, the degree over $\mathbb{Q}$ of $\mathbb{Q}(i)$ is 2, and 5, 2 are relatively prime. Hence the field $\mathbb{Q}(i, \alpha)$ has degree 10 over $\mathbb{Q}$, which implies that it has degree 5 over $\mathbb{Q}(i)$. Therefore $x^5 - 4x + 2$ is the minimal polynomial of α over $\mathbb{Q}(i)$: it is irreducible over $\mathbb{Q}(i)$.

The polynomial $x^4 - 4x + 2$ has two real roots (one < 1 and one > 1). Let β be one of them. The field $\mathbb{Q}(\beta)$ is contained in $\mathbb{R}$, hence it does not contain i, and i has degree 2 over $\mathbb{Q}(\beta)$. The field $\mathbb{Q}(i, \beta)$ has degree 8 over $\mathbb{Q}$ and 4 over $\mathbb{Q}(i)$, which implies that the polynomial $x^4 - 4x + 2$ is the minimal polynomial of β over $\mathbb{Q}(i)$: it is irreducible over $\mathbb{Q}(i)$.

- Problem 5.11 p. 53.

Set $y = x - 1$. We have

$$1 + x + \cdots + x^{p-1} = \frac{x^p - 1}{x - 1} = \frac{(y+1)^p - 1}{y} = p + \frac{p(p-1)}{2}y + \frac{p(p-1)(p-2)}{6}y^2 + \cdots + py^{p-1} + y^p.$$

Each coefficient apart from the leading one is divisible by p:

$$p \text{ divides } \frac{p!}{(p-j)!j!} = \frac{p(p-1)\cdots(p-j+1)}{j!} \text{ for } 1 \leq j \leq p-1$$

and the constant coefficient p is not divisible by p^2. Hence, by Eisenstein's Criterion, this polynomial is irreducible in $\mathbb{Q}[y]$, from which the desired result follows.

- Problem 5.12 p. 53.

Let $\alpha = e^{i\theta}$ with $\theta = 2\pi/7$. We have $\alpha^7 = 1$ and $\alpha \neq 1$, hence α is a root of the polynomial

$$f(x) = \frac{x^7 - 1}{x - 1} = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6.$$

From Problem 5.11 we deduce that this polynomial is irreducible over $\mathbb{Q}$, hence it is the minimal polynomial of α over $\mathbb{Q}$.

We have $2\alpha = \cos\theta + i\sin\theta$ and $\cos\theta = \alpha + \alpha^{-1}$. This last relation shows that α is root of the quadratic polynomial $x^2 - x\cos\theta + 1 \in \mathbb{Q}(\cos\theta)[x]$, hence α is algebraic of degree ≤ 2 over $\mathbb{Q}(\cos\theta)$. Notice that $\cos\theta \in \mathbb{R}$ and $\alpha \notin \mathbb{R}$, hence $\mathbb{Q}(\cos\theta) \neq \mathbb{Q}(\alpha)$ and therefore $[\mathbb{Q}(\alpha) : \mathbb{Q}(\cos\theta)] = 2$. From

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\cos\theta)][\mathbb{Q}(\cos\theta) : \mathbb{Q}],$$

we deduce $[\mathbb{Q}(\cos\theta) : \mathbb{Q}] = 3$.

Since the polynomial f is reciprocal: $f(x) = x^6 f(1/x)$, it follows that there exists a polynomial $g \in \mathbb{Q}[y]$ such that $f(x) = x^3 g(x + x^{-1})$. Writing

$$y = x + x^{-1}, \quad x^2 + x^{-2} = y^2 - 2, \quad x^3 + x^{-3} = y^3 - 3y,$$

we obtain the irreducible polynomial of $2\cos\theta$ over $\mathbb{Q}$:

$$g(y) = y^3 + y^2 - 2y - 1.$$

• Problem 6.4 p. 57.

Using simple geometric constructions, one proves:

• (x, y) is constructible if and only if $(x, 1)$ and $(y, 1)$ are constructible.

• If (x, y) is constructible, then $(x + y, 1)$ and $(xy, 1)$ are constructible.

• If $(x, 1)$ is constructible and $x \neq 0$, then $(1/x, 1)$ is constructible.

As a consequence, the set L of $x \in \mathbb{R}$ such that $(x, 1)$ is constructible is a subfield of $\mathbb{R}$, and the set of constructible points is $L \times L$.

The answer to Problem 6.4 follows from these remarks.

• Problem 6.5 p. 57.

The degree over $\mathbb{Q}$ of the field $\mathbb{Q}(2^{1/3})$ is 3, not a power of 2, hence Theorem 6.1 shows that it is not possible to duplicate the cube.

• Problem 6.6 p. 57.

The polynomial $x^9 - 1$ splits as

$$(x^3 - 1)(x^6 + x^3 + 1) = (x - 1)(x^2 - x + 1)(x^6 + x^3 + 1).$$

The number $e^{2i\pi/9}$ is a root of the polynomial $f(x) = x^6 + x^3 + 1$. Set $y = x - 1$. Then

$$f(y + 1) = y^6 + 6y^5 + 15y^4 + 21y^3 + 18y^2 + 9y + 3,$$

which is irreducible by Eistenstein criterion for $p = 3$. Therefore $e^{2i\pi/9}$ has degree 6 over $\mathbb{Q}$, not a power of 2.

From Problem 5.11 we deduce that the number $e^{2i\pi/7}$ has also degree 6 over $\mathbb{Q}$.

Therefore (Theorem 6.1) $e^{2i\pi/9}$ and $e^{2i\pi/7}$ are not constructible; the regular nonagon and the regular heptagon cannot be constructed using ruler and compasses.

• Problem 6.7 p. 58.

(a) It has been explained in § 6.1 that any point $(r_1, r_2) \in \mathbb{Q}^2$ can be constructed (this follows also from Problem 6.4, say with $P = (1, 0)$). Assume K is a subfield of $\mathbb{R}$ such that any point in K^2 can be constructed. Let $(x, y) \in \mathbb{R}^2$ such that $[K(x, y) : K] = 2$. Solving the quadratic equation, there is a number $d \in K$ such that x and y are of the form $a + b\sqrt{d}$ with a and b in K. Since $(d, 1)$ is constructible, also $(\sqrt{d}, 1)$ is constructible. From Problem 6.4 it follows that all points of the form $(a + b\sqrt{d}, 1)$ with a and b in K are constructible. One deduces that (x, y) is constructible.

(b) follows from (a) by induction.