Yale University Department of Mathematics
Math 370 Fields and Galois Theory
Spring 2018

Problem Set # 4 (due in class on Thursday 15 February)

Notation: For a positive integer n, write $\zeta_n = e^{2\pi i/n} \in \mathbb{C}$.

Reading: GT 7.

Problems:

1. GT Exercise 7.3.
This is more of a historically interesting problem. We will prove that a general angle cannot be trisected using compass and straightedge. However, this shows you that if you have a "marked ruler" then you can trisect an angle. So the exact rules you are allowed to use in making compass and straightedge constructions are very important!

2. Let p be an odd prime. Prove that $\mathbb{Q}(\zeta_p)$ has degree $p-1$ over $\mathbb{Q}$. Prove that $\mathbb{Q}(\cos(2\pi/p))$ has degree $(p-1)/2$ over $\mathbb{Q}$.
Hint. These are related.

3. For $1 \le n \le 8$ find the minimal polynomial $\Phi_n(x)$ of ζ_n over $\mathbb{Q}$. For each $1 \le n \le 8$ compute $\prod_{d|n} \Phi_d(x)$, where the product is taken over all divisors of n (including 1 and n).

4. Determine the splitting field over $\mathbb{Q}$, in the form $\mathbb{Q}(\alpha_1, \dots, \alpha_n)$ for explicit $\alpha_i \in \mathbb{C}$, as well as its degree over $\mathbb{Q}$, for each of the following polynomials:

(a) $x^3 - 1$

(b) $x^4 + 5x^2 + 6$

(c) $x^6 - 8$

5. Let F be a field and let $g(x) = x^2 + bx + c \in F[x]$. Let K be the spitting field of g, so that $g(x) = (x-\alpha)(x-\beta)$ over K, for elements $\alpha, \beta \in K$.

(a) Prove that $(\alpha - \beta)^2 = b^2 - 4c \in F$. This is called the **discriminant** $\Delta(g)$ of the monic quadratic polynomial g.
Hint. Use elementary symmetric polynomials.

(b) Prove that $\Delta(g) = 0$ if and only if g has repeated roots in K (i.e., α, β are not distinct).

(c) Assume that the characteristic of F is not 2. Prove that $K = F(\sqrt{\Delta(g)})$. Deduce that $g(x)$ is irreducible over F if and only if $\Delta(g)$ is not a square in F. Also, prove that $g(x)$ is a square in $F[x]$ if and only if $\Delta(g) = 0$.
Hint. You are free to use the quadratic formula.

(d) Now let $F = \mathbb{F}_2(t)$ be the rational function field over $\mathbb{F}_2$. Let $g(x) = x^2 - t \in F[x]$. Prove that $g(x)$ is irreducible over F, though it satisfies $\Delta(g) = 0$. Show that the splitting field of $g(x)$ is the field extension $K = F(\sqrt{t}) := F[x]/(g(x))$ and find the roots of $g(x)$ over K. We don't know it yet, but K/F is called an inseparable quadratic extension.
Hint. First year's dream!

Weird stuff can happen with quadratic polynomials in characteristic 2!

6. Let F be a field and let $f(x) = x^3 + px + q \in F[x]$. Let L be the spitting field of f, so that $f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ over L, for elements $\alpha_1, \alpha_2, \alpha_3 \in L$.

(a) Prove that $\prod_{1 \le i < j \le 3} (\alpha_i - \alpha_j)^2 = -4p^3 - 27q^2 \in F$. This is called the **discriminant** $\Delta(f)$ of the monic cubic polynomial f.
Hint. Use elementary symmetric polynomials.

(b) Prove that $\Delta(f) = 0$ if and only if f has repeated roots in L (i.e., $\alpha_1, \alpha_2, \alpha_3$ are not distinct).

(c) Let $\alpha \in L$ be one of the roots of $f(x)$. Factor $f(x) = (x - \alpha)g(x)$ over $F(\alpha)$, where $g(x) \in F(\alpha)[x]$ is quadratic. Prove that $\Delta(f) = g(\alpha)^2 \Delta(g)$.

(d) Assume that the characteristic of F is not 2 and let α be a root of $f(x)$. Prove that $L = F(\alpha, \sqrt{\Delta(f)})$. Deduce that if $\Delta(f)$ is a square in F then L has degree at most 3 over F, in particular, if $f(x)$ is reducible over F, then $L = F(\sqrt{\Delta(f)})$.

(e) Write down a monic irreducible cubic polynomial over $\mathbb{F}_3(t)$ whose discriminant is 0, and factor it over its splitting field.
Hint. Think inseparable.

(f) Now let $F = \mathbb{F}_2(t)$ and let $f(x) = x^3 + tx + t$. Prove that $f(x)$ is irreducible over F, has nonzero square discriminant, yet its splitting field L has degree 6 over F.
Hint. You may find it useful to use Gauss's Lemma for the ring $F[t]$, see Dummit and Foote, §9.3.

Weird stuff can happen with cubic polynomials in characteristics 2 and 3!