Dartmouth College Department of Mathematics
Math 81/111 Abstract Algebra
Winter 2025

Problem Set # 4 (due via Canvas upload by midnight Friday 7 February)

Problems:

1. Let F be a field and $f(x) \in F[x]$ a monic polynomial of degree n. Let E be a splitting field of f over F, so that $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ over E.

(a) Prove that $\prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2$ is in F. This is called the **discriminant** $\Delta(f)$ of f. **Hint.** You might need the Fundamental Theorem of Symmetric Polynomials.

(b) Prove that $\Delta(f) = 0$ if and only if $f(x)$ has a repeated root in E.

(c) Prove that if Δ is not a square in F then $[E : F]$ is even. **Hint.** The tower law.

2. Let F be a field and let $g(x) = x^2 + ax + b \in F[x]$. Let $K = F(\alpha)$, where α is a root of $g(x)$, so that $g(x) = (x - \alpha)(x - \beta)$ over K. This problem is mostly review of what you already know about quadratic polynomials, so you don't need to write much!

(a) Prove that $\Delta(g) = (\alpha - \beta)^2 = a^2 - 4b \in F$. **Hint.** Use elementary symmetric polynomials.

(b) 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.** Use the quadratic formula.

(c) 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 $\Delta(g) = 0$. Recall, from lecture, that $K \cong F(\sqrt{t})$ is an example of an inseparable extension (though in lecture we only indicated how to prove the irreducibility of $g(x)$). **Hint.** Proving irreducibility can either go like proving $\sqrt{2}$ is irrational, or using Eisenstein for the ring $\mathbb{F}_2[t]$.

Weird stuff can happen with quadratic polynomials in characteristic 2!

3. Let F be a field and let $f(x) = x^3 + px + q \in F[x]$. Let L be the splitting 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 $\Delta(f) = \prod_{1 \le i < j \le 3} (\alpha_i - \alpha_j)^2 = -4p^3 - 27q^2 \in F$.

(b) 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 $\Delta(f) = g(\alpha)^2 \Delta(g)$.

(c) Assume that the characteristic of F is not 2. If $f(x)$ is irreducible and α is a root of $f(x)$, prove that $L = F(\alpha, \sqrt{\Delta(f)})$. Deduce that, in this case, $\Delta(f)$ is a square in F if and only if L has degree 3 over F. If $f(x)$ is reducible over F, prove that $L = F(\sqrt{\Delta(f)})$; for this, you cannot necessarily just assume that the root α is in F in the previous case..

(d) Assume that the characteristic of F is not 2 or 3. Prove that if $\Delta(f) = 0$ then $L = F$, i.e., all the roots of $f(x)$ are in 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. Write down a monic cubic polynomial over $\mathbb{F}_2(t)$ whose discriminant is 0, and whose splitting field is nontrivial. **Hint.** Think inseparably.

(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!

4. Let p and q be distinct prime numbers. Prove that $\mathbb{Q}(\sqrt{p}+\sqrt{q}) = \mathbb{Q}(\sqrt{p}, \sqrt{q})$ and find the minimal polynomial of $\sqrt{p}+\sqrt{q}$ over $\mathbb{Q}$.

5. Let F be a field of characteristic $\neq 2$.

(a) Let $a_1, \dots, a_n \in F$ be distinct elements such that no product $a_{i_1} \cdots a_{i_r}$, with distinct indices i_j, is a square in F. Prove that $K = F(\sqrt{a_1}, \dots, \sqrt{a_n})$ has degree 2^n over F.

(b) Prove that the field $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11}, \dots)$ gotten by adjoining the square roots of all prime numbers to $\mathbb{Q}$, is an infinite degree algebraic extension of $\mathbb{Q}$.

Dartmouth College, Department of Mathematics, 6188 Kemeny Hall, Hanover, N.H. 03755
E-mail address: asher.auel@dartmouth.edu