Yale University Department of Mathematics
Math 370 Fields and Galois Theory
Spring 2019

Problem Set # 5 (due in class on Thursday February 28)

Notation: Let K and L be subfields of a field M. The **compositum** of K and L, denoted KL, is defined to be the smallest subfield of M containing both K and L, equivalently, the intersection of all subfields of M containing K and L. If additionally K and L are both extensions of a field F, we say that the extensions K/F and L/F are **linearly disjoint** if any F-linearly independent subset of K is L-linearly independent in KL and if any F-linearly independent subset of L is K-linearly independent in KL.

Problems:

1. Let F be a field and K/F and L/F be subextensions of a field extension M/F.

(a) Prove that if $K = F(\alpha_1, \dots, \alpha_n)$ and $L = F(\beta_1, \dots, \beta_m)$ are finitely generated, then $KL = F(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m)$.

(b) Prove that if K/F and L/F are finite then KL/F is finite and $[KL : F] \leq [K : F]\,[L : F]$ with equality if and only if K/F and L/F are linearly disjoint.
Hint. Prove that if $x_1, \dots, x_n$ is an F-basis for K and $y_1, \dots, y_m$ is an F-basis for L, then the products $x_i y_j$ for $1 \leq i \leq n$ and $1 \leq j \leq m$ span KL/F and are an F-basis if and only if K/F and L/F are linearly disjoint.

(c) Prove that finite extensions K/F and L/F of relatively prime degree are linearly disjoint. (Now you can do Problem 5a on Midterm 1 easily!)

(d) Let $f(x)$ be an irreducible polynomial over F and K/F a finite extension. Prove that if $\deg(f)$ and $[K : F]$ are relatively prime, then $f(x)$ is still irreducible over K.
This is a generalization of Problem 7 on Problem set 4. **Hint.** Use the previous part.

(e) Prove that if K/F and L/F are linearly disjoint then $K \cap L = F$. Find an example showing that the converse is false.

2. Let F be a field, $f(x)$ a polynomial over F with splitting field E/F.

(a) Let K/F be a subextension of E/F. Prove that E/K is a splitting field of $f(x)$ considered as a polynomial over K.

(b) Prove that if $\deg(f) = n$ then $[E : F]$ divides $n!$. (We only had $[E : F] \leq n!$ before.)
Hint. Use induction on n, and deal with cases of f reducible or irreducible separately. At some point you'll need the fact that $a!b!$ divides $(a+b)!$, which you should also prove.

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

(a) Prove that $\prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 \in F$. This is called the **discriminant** $\Delta(f)$ of f.
Hint. Remember the Vandermonde and the elementary 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.

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

(a) Prove that $\Delta(f) = -4p^3 - 27q^2$. **Hint.** Use elementary symmetric polynomials.

(b) Let $\alpha \in E$ 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 and let α be a root of $f(x)$. Prove that $E = F(\alpha, \sqrt{\Delta(f)})$. Deduce that if $\Delta(f)$ is a square in F then E has degree at most 3 over F, in particular, if $f(x)$ is reducible over F, then $E = F(\sqrt{\Delta(f)})$.

(d) 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. You've already seen this.

(e) 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 E has degree 6 over F.
Hint. As before, use the Eisenstein criterion and Gauss's lemma for polynomials over the ring $\mathbb{F}_2[t]$.

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

5. Let $F \subset \mathbb{R}$ be a subfield and $f(x) \in F[x]$ a cubic polynomial with discriminant Δ.

(a) You know that $\Delta = 0$ if and only if $f(x)$ has a repeated root. Prove that in this case, all the roots of $f(x)$ are in F.

(b) Prove that $\Delta > 0$ if and only if all the roots of $f(x)$ are real.

(c) Prove that $\Delta < 0$ if and only if $f(x)$ a single real root and a pair of complex conjugate roots.

Try to think of what these conditions mean for polynomials of higher odd degree (e.g., degree 5).