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

Problem Set # 2 (due in class on Thursday 1 February)

Notation: Let F be a field. A field extension K/F is **simple** if $K = F(\alpha)$ for some $\alpha \in K$. See GT 4.3 for details.

Reading: GT 3,4.

Problems:

1. GT Exercise 4.3.
Here, you start getting hands-on practice with field extensions. "Describe" is a vague term. The point is for you to play with some extensions and think about their structure. In this one problem, you do not have to prove your claims, you do not have to find explicit formulas for inverses, or anything like that. Just consider each field and write down what you think it's like. For the finite extensions, you should find the basis as a vector space over the ground field, and list all proper subfields that you can think of (again, no proof needed). In part (f) and (g), you'll confront the notion of transcentantal extensions (which have infinite degree).

2. GT Exercise 4.4.

3. GT Exercise 4.5.
Be careful: remember that simple extension are not necessarily finite!

4. Let $\alpha \approx -1.7693$ be the real root of $x^3 - 2x + 2$. In the extension $\mathbb{Q}(\alpha)/\mathbb{Q}$, write the element $(\alpha + 1)^{-1}$ explicitly as a polynomial in α with coefficients in $\mathbb{Q}$.

5. Prove that the fields $\mathbb{Q}[x]/(x^2 - 4x + 2)$ and $\mathbb{Q}(\sqrt{2})$ are isomorphic as extensions of $\mathbb{Q}$.

6. Let F be a field of characteristic $\neq 2$ and let K/F be a field extension of degree 2. Prove that there exists $\alpha \in K$ with $\alpha^2 \in F$ such that $K = F(\alpha)$.

7. Factor the following polynomials in $\mathbb{Q}[x]$, using reduction mod 2:

(a) $x^2 + 2345x + 125$
(b) $x^3 + 5x^2 + 10x + 5$
(c) $x^4 + 2x^3 + 2x^2 + 2x + 2$
(d) $x^4 + 2x^3 + 3x^2 + 2x + 1$
(e) $x^5 + x^4 - 4x^3 + 2x^2 + 4x + 1$

8. The goal is to prove that $f(x) = x^4+1$ is reducible modulo every prime number p. You already know (PS#1) that $f(x)$ irreducible over $\mathbb{Q}$, and here you'll give a different proof (probably).

(a) Factor $f(x)$ modulo 2.
(b) Assume that $-1 = u^2$ is a square in $\mathbb{F}_p$. Then use the equality $x^4 + 1 = x^4 - u^2$ to factor $f(x)$ modulo p.
(c) Assume that p is odd and $2 = v^2$ is a square in $\mathbb{F}_p$. Then use the equality $x^4 + 1 = (x^2 + 1)^2 - (vx)^2$ to factor $f(x)$ modulo p.
(d) Prove that if p is odd and neither -1 nor 2 is a square in $\mathbb{F}_p$, then -2 is a square. Use this to factor $f(x)$ modulo p.
(e) Prove that $f(x)$ is irreducible over $\mathbb{Z}$ by using the Eisenstein criterion. **Hint.** Use the same trick that works for $x^4 + x^3 + x^2 + x + 1$.