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

Problem Set # 2 (due in class on Thursday 31 January)

Notation: Let F be a field. As defined in FG p. 13, if K and K' are field extensions of F, an F-homomorphism $\varphi : K \to K'$ is a ring homomorphism such that $\varphi(c) = c$ for all $c \in F$. An F-isomorphism of field extensions is a bijective F-homomorphism.

Reading: FT pp. 11–17

Problems:

1. The goal is to prove that $f(x) = x^4+1 \in \mathbb{Z}[x]$ is reducible modulo every prime number p. You already know (PS#1) that $f(x)$ irreducible, 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. Conclude that x^4+1 is reducible modulo every prime p.

(e) Prove that $f(x)$ is irreducible by using the Eisenstein criterion. **Hint.** Use the same trick that works for $x^4 + x^3 + x^2 + x + 1$.

2. Assume that for some prime number p, the reduction of a monic polynomial $f(x) \in \mathbb{Z}[x]$ factors into a product $\overline{f}(x) = \overline{g}(x)\overline{h}(x)$ of monic irreducible polynomials in $\mathbb{F}_p[x]$. Prove that if $f(x)$ is reducible in $\mathbb{Z}[x]$, then it must factor into a product $f(x) = g(x)h(x)$ of monic irreducible polynomials $g(x), h(x) \in \mathbb{Z}[x]$ that reduce to $\overline{g}(x), \overline{h}(x) \in \mathbb{F}_p[x]$, respectively.

Use this idea to 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) $x^5 + x^4 - 4x^3 + 2x^2 + 4x + 1$

3. Let K and K' be field extensions of a field F.

(a) Prove that any F-homomorphism $\varphi : K \to K'$ is injective.

(b) Prove that if K'/F is finite and $\varphi : K \to K'$ is an F-homomorphism, then K/F is finite.

(c) Assume that both K and K' are finite over F, and that $\varphi : K \to K'$ is an F-homomorphism. The φ is an F-isomorphism if and only if $[K : F] = [K' : F]$.

(d) Prove that $f(x) = x^2 - 4x + 2 \in \mathbb{Q}[x]$ is irreducible, hence the quotient ring $K = \mathbb{Q}[x]/(f(x))$ is a field extension of $\mathbb{Q}$ by FT p. 16. Prove that the extensions K and $\mathbb{Q}(\sqrt{2})$ of $\mathbb{Q}$ are $\mathbb{Q}$-isomorphic and exhibit an explicit F-isomorphism between them.

4. At the end of this problem, prove that $\mathbb{Q}(\sqrt{2}, i)$ and $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ have degree 4 over $\mathbb{Q}$.

(a) Prove that the complex numbers $1, \sqrt{2}, i, \sqrt{2}i$ are linearly independent over $\mathbb{Q}$.
Hint. Use real and imaginary considerations.

(b) Prove that the real numbers $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ are linearly independent over $\mathbb{Q}$.
Hint. Show that a dependence would imply $\sqrt{3} = a + b\sqrt{2}$, then square both sides.

5. 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 $\mathbb{Q}$.