Dartmouth College Department of Mathematics

Math 81/111 Abstract Algebra

Winter 2020

Problem Set # 2 (due in class on Friday 24 January)

Notation: Let F be a field. As defined in FT 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: DT 13.1–13.4, FT pp. 11–23

Problems:

1. *Subgroups of fields.* Let F be a field.

(a) Let G be a finite abelian group. Prove that G is cyclic if and only if G has at most m elements of order dividing m for each $m \mid \#G$. Hint. You'll need the structure theorem of finite abelian groups.

(b) Prove that every finite subgroup G of the multiplicative group $F^\times = F \smallsetminus \{0\}$ is cyclic. Hint. Use the fact that a polynomial of degree m has at most m roots in F.

(c) Deduce that if F is a finite field then $F^\times$ is cyclic. For each field F having at most 7 elements, find an explicit generator of $F^\times$.

(d) Prove that for any odd prime p, the set of nonzero squares is an index 2 subgroup of $\mathbb{F}_p^\times$.

2. 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 in $\mathbb{Q}[x]$.

(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. In this case, factor $f(x)$ modulo any such p. Hint. For the first part, use the previous problem.

(e) Conclude that $x^4 + 1$ is reducible modulo every prime p.

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. Let $\alpha \approx -1.7693$ be the real root of $x^3 - 2x + 2$. In the extension $\mathbb{Q}(\alpha)/\mathbb{Q}$, write the elements α^{-1} and $(\alpha+1)^{-1}$ explicitly as a polynomial in α with coefficients in $\mathbb{Q}$. (Look up the algorithm using the Bezout identity on FT p. 16.)

5. Let F be a field of characteristic $\neq 2$ and let K/F be a field extension of degree 2.

(a) Prove that there exists $\alpha \in K$ with $\alpha^2 \in F$ such that $K = F(\alpha)$. We often write $\alpha = \sqrt{a}$ if $\alpha^2 = a \in F$. Hint. Get inspiration from the quadratic formula.

(b) For $a, b \in F^\times$ prove that $F(\sqrt{a}) \cong F(\sqrt{b})$ if and only if $a = u^2 b$ for some $u \in F^\times$.

(c) Deduce that there is a bijection between the set of F-isomorphism classes of field extensions K/F with $[K : F] \mid 2$ and the group $F^\times/F^{\times 2}$ of units in F modulo squares.

(d) If F is a finite field of characteristic $\neq 2$, prove that F has a unique quadratic extension (up to F-isomorphism).

6. For each extension K/F and each element $\alpha \in K$, find the minimal polynomial of α over F (and prove that it is the minimal polynomial).

(a) i in $\mathbb{C}/\mathbb{R}$ (b) i in $\mathbb{C}/\mathbb{Q}$ (c) $(1+\sqrt{5})/2$ in $\mathbb{R}/\mathbb{Q}$ (d) $\sqrt{2+\sqrt{2}}$ in $\mathbb{R}/\mathbb{Q}$

7. Let $\pi \in \mathbb{R}$ be the area of a unit circle and let $\alpha = \sqrt{\pi^2 + 2}$. Consider the field $K = \mathbb{Q}(\pi, \alpha)$. For the following field extensions, determine whether they are transcendental and/or algebraic and/or finite and/or simple, and if you determine the extension is simple and algebraic, find a simple generator and determine its minimal polynomial.

(a) $K/\mathbb{Q}$ (b) $K/\mathbb{Q}(\pi)$ (c) $K/\mathbb{Q}(\alpha)$ (d) $K/\mathbb{Q}(\pi + \alpha)$

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