

DARTMOUTH COLLEGE DEPARTMENT OF MATHEMATICS
Math 81/111 Abstract Algebra: Field and Galois Theory
Winter 2025

Problem Set # 2 (due by Canvas upload by the end of Friday 24 January)

Notation: Let F be a field. If K and K' are field extensions of F , an F -homomorphism $\varphi : K \rightarrow K'$ is a unital ring homomorphism such that $\varphi(c) = c$ for all $c \in F$, i.e., φ is a unital F -algebra homomorphism (cf. see FT p. 14). An F -isomorphism of field extensions is an invertible F -homomorphism.

We say that a field extension K/F is algebraic if every element $\alpha \in K$ is algebraic over F . We will see that any field extension generated by algebraic elements is itself algebraic.

Reading: DT 13.1–13.4, FT pp. 11–21

Problems:

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

- 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.** One possible proof uses the structure theorem of finite abelian groups, but you can get away with slightly less.
- Prove that every finite subgroup G of the multiplicative group $F^\times = F \setminus \{0\}$ is cyclic. **Hint.** Use the fact that a polynomial of degree m has at most m roots in F .
- 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 .
- Let p be an odd prime. Prove that $-1 \in \mathbb{F}_p^\times$ is a square if and only if $p \equiv 1 \pmod{4}$.
- Prove that for any odd prime p , the set of nonzero squares is an index 2 subgroup of \mathbb{F}_p^\times . **Hint.** You can use the above results, but there's also a purely combinatorial proof.

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 (HW#1) that $f(x)$ is irreducible in $\mathbb{Q}[x]$.

- Factor $f(x)$ modulo 2.
- 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 .
- 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 .
- 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.
- Conclude that $x^4 + 1$ is reducible modulo every prime p .

3. Let K and K' be field extensions of a field F .
- Prove that any F -homomorphism $\varphi : K \rightarrow K'$ is injective.
 - Prove that if K'/F is finite and $\varphi : K \rightarrow K'$ is an F -homomorphism, then K/F is finite.
 - Assume that both K and K' are finite over F , and that $\varphi : K \rightarrow K'$ is an F -homomorphism. The φ is an F -isomorphism if and only if $[K : F] = [K' : F]$.
 - Prove that $f(x) = x^2 - 4x + 2 \in \mathbb{Q}[x]$ is irreducible. Prove that the extensions $K = \mathbb{Q}[x]/(f(x))$ and $\mathbb{Q}(\sqrt{2})$ of \mathbb{Q} are \mathbb{Q} -isomorphic and exhibit an explicit \mathbb{Q} -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} . **Hint.** Remember the algorithm using the Bezout identity (e.g., FT p. 16–17).
5. 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 $K = F(\alpha)$. We often write $\alpha = \sqrt{a}$ if $\alpha^2 = a \in F$. **Hint.** Get inspiration from the quadratic formula.
 - For $a, b \in F^\times$ prove that $F(\sqrt{a}) \cong F(\sqrt{b})$ if and only if $a = u^2b$ for some $u \in F^\times$.
 - 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.
 - 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).
- i in \mathbb{C}/\mathbb{R}
 - i in \mathbb{C}/\mathbb{Q}
 - $(1 + \sqrt{5})/2$ in \mathbb{R}/\mathbb{Q}
 - $\sqrt{2 + \sqrt{2}}$ 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.
- K/\mathbb{Q}
 - $K/\mathbb{Q}(\pi)$
 - $K/\mathbb{Q}(\alpha)$
 - $K/\mathbb{Q}(\pi + \alpha)$