Algebra II: Homework 12

Due on April 28, 2021

Professor Walton

Gabriel Gress

Last edited April 28, 2021

Problem 1

Claim. Factor $x^8 - x$ into irreducibles in $\mathbb{Z}[x]$ and in $\mathbb{F}_2[x]$.

Proof. $\mathbb{Z}[x]$:

$$x^8 - x = x(x^7 - 1) = x(x-1)(1 + x + x^2 + x^3 + x^4 + x^5 + x^6)$$

which is clearly all irreducible terms. But in $\mathbb{F}_2[x]$:

$$x(x-1)(1 + x + x^2 + \ldots + x^6) = x(x-1)(1 + x^2 + x^3)(1 + x + x^3).$$

□

Problem 2

Claim. Prove that an algebraically closed field must be infinite.

Proof. Let $F = \{a_1, \ldots, a_n\}$ be a finite field. Consider the polynomial

$$p(x) = (x - a_1)(x - a_2)\ldots(x - a_n) + 1_F$$

It is easy to see that $p(x) = 1$ for all $x \in F$, and hence has no roots in F. Therefore, F cannot be algebraically closed if it is finite. □

Problem 3

Claim. Determine the Galois closure of the field $\mathbb{Q}(\sqrt{1+\sqrt{2}}$ over $\mathbb{Q}$.

Proof. First we will find the minimal polynomial, and then take its splitting field to be the Galois closure. Observe that for $x = \sqrt{1+\sqrt{2}}$:

$$x^4 - 2x^2 - 1 = 0$$

and because we are in $\mathbb{Q}$, this must be the minimal degree for which this holds. Now we verify that p is separable. By the quadratic formula, the roots of

$$p(x) = x^4 - 2x^2 - 1$$
$$x_1, x_2 = \pm\sqrt{1+\sqrt{2}}$$
$$x_3, x_4 = \pm i\sqrt{-1+\sqrt{2}}$$

and hence p is separable. Thus the Galois closure is its splitting field, and hence must be

$$\mathbb{Q}(\sqrt{1+\sqrt{2}}, i\sqrt{-1+\sqrt{2}}).$$

□

Problem 3 continued on next page...

Problem 4

Claim. Let $q = p^m$ be a power of the prime p and let $\mathbb{F}_q = \mathbb{F}_{p^m}$ be the finite field with q elements. Let $\sigma_q = \sigma_p^m$ be the m-th power of the Frobenius automorphism σ_p, called the q-Frobenius automorphism.

(a). Prove that σ_q fixes $\mathbb{F}_q$.

(b). Prove that every finite extension of $\mathbb{F}_q$ of degree n is the splitting field of $x^{q^n} - x$ over $\mathbb{F}_q$, and hence is unique.

(c). Prove that every finite extension of $\mathbb{F}_q$ of degree n is cyclic with σ_q as generator.

(d). Prove that the subfields of the unique extension of $\mathbb{F}_q$ of degree n are in bijective correspondence with the divisors d of n.

Proof. (a). Let $x \in \mathbb{F}_q$ be given. Then

$$\sigma_q(x) = x^p \cdot_{m \text{ times}} \cdot x^p = x^{p^m}$$

But $x^{p^m} - x = 0$, so $x^{p^m} = x$, and hence $\sigma_p(x) = x$ for all $x \in \mathbb{F}_q$, as desired.

(b). Let $K/\mathbb{F}_q$ be a finite extension with degree n. By the tower formula:

$$[K : \mathbb{F}_p] = [K : \mathbb{F}_q][\mathbb{F}_q : \mathbb{F}_p] = nm$$

and hence is a degree nm extension of $\mathbb{F}_p$. This tells us it is the splitting field of

$$x^{p^n m} = x^{q^n}$$

as desired.

(c). Let K be a finite extension of $\mathbb{F}_q$ and a be the order of σ_q so that $\sigma_q^a = 1_K$. Then it holds that $\sigma_q^a(k) = k = k^{q^a}$. Our goal is to show that $a = n$ and hence σ_q is a cyclic generator. It already must hold that $a \leq n$. Now consider

$$k^{q^a} - k = 0.$$

This has exactly q^n zeroes as $K := \mathbb{F}_{p^{q^n}}$. Hence $a \geq n$, which gives us that $a = n$, as desired.

(d). By the above work we can see that the subfields of $\mathbb{F}_q$ correspond to subgroups of the Galois group. The correspondence is unique by part (b), and by part (c) we know that the subgroups are cyclic groups and hence the order must divide n.

□

Problem 5

Claim. Let $f(x) \in F[x]$ be an irreducible polynomial of degree n over the field F, let L be the splititng field of $f(x)$ over F and let α be a root of $f(x)$ in L. If K is any Galois extension of F, show that the polynomial $f(x)$ splits into a product of m irreducible polynomials each of degree d over K, where

$$d = [K(\alpha) : K] = [(L \cap K)(\alpha) : L \cap K]$$
$$m = n/d = [F(\alpha) \cap K : F].$$

Problem 5 continued on next page...

Proof. First we will show that the factorization of $f(x)$ over K is the same as its factorization over $L \cap K$. Let

$$f = \prod_{i \in I} f_i$$

be a factorization of f into polynomials f_i that are irreducible in K. By construction, f is algebraic in L and so f_i are all linear factors and hence are elements of $L[x]$. Then by irreducibility theorems, we have that f_i is irreducible in $K \cap L$ if and only if it is irreducible in K, and hence must share the same factorization.

Let H be the subgroup of the Galois group of L over F that corresponds to $L \cap K$. The factors of $f(x)$ over $L \cap K$ correspond to the orbits of H on the roots of $f(x)$. By Exercise 9 of Section 4.1, these orbits all have order d, where d is the degree of f_i over K. Thus

$$d = [K(\alpha) : K] = [(L \cap K)(\alpha) : (L \cap K)].$$

By definition of m, we have that $m = \frac{n}{d}$ and hence

$$m = \frac{n}{d} = \frac{[F(\alpha) : F]}{[F(\alpha) : F(\alpha) \cap K]} = [F(\alpha) \cap K : F].$$

□

Problem 6

Claim. Let p be a prime and F a field. Let K be a Galois extension of F whose Galois group is a p-group. Such an extension is called a p-extension.

(a). Let L be a p-extension of K. Prove that the Galois closure of L over F is a p-extension of F.

(b). Give an example to show that (a) need not hold if $[K : F]$ is a power of p but K/F is not Galois.

Proof. (a).

(b). Consider $K/F = \mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. We have previously shown that K/F is not Galois, and that $[K : F] = 2$. It has minimal polynomial given by

$$p(x) = x^3 - 2.$$

The Galois extension is $\overline{L} = \mathbb{Q}(\sqrt[3]{2}, \sqrt{3}i)$ which satisfies $[\overline{L} : F] = 6$ by the tower theorem. Hence it is not a prime power.

□

Problem 7

Claim. Verify that $\mathbb{Q}(\sqrt[3]{2})$ is not a subfield of any cyclotomic field over $\mathbb{Q}$.

Proof. Let ω be an arbitrary k-th root of unity. Suppose that $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\omega)$ for some choice of ω, for the sake of contradiction. We know that $\mathbb{Q}(\omega)$ is Galois and hence $\mathrm{Gal}(\mathbb{Q}(\omega))$ is abelian. Thus $\overline{Q(\sqrt[3]{2}) \subset Q(\omega)}$. But we have that Galois group of the extension of $x^3 - 2$ is isomorphic to S_3, which is non-abelian, and

Problem 7 continued on next page...

hence cannot be contained in the abelian group above.

This works by the fundamental theorem– choose $F = \mathbb{Q}$, $E = \mathbb{Q}(\sqrt[3]{2})$, and $K = Q(\omega)$ and apply that $F \subset E \subset K$, $\mathbb{Q}(\sqrt[3]{2})$ Galois over $\mathbb{Q}$ implies

$$\begin{aligned} \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) &\cong \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})/\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}(\sqrt[3]{2})) \\ &\implies \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) \subset \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \end{aligned}$$

□