Galois Thy: GAL #09

Due on Apr 29, 2022 at 11:59pm

Prof Matyas Domokos Sec 12 & 13

Xianzhi

2023

HW09
Apr 29, 2022
Exercise 12.4.11
Exercise 13.3.3
Exercise 13.3.5

Problem 1

Exercise 12.4.8 Factor $x^4 + x + 1 \in \mathbb{F}_2[x]$ as a product of irreducibles over $\mathbb{F}_4$.

Soln:

Problem 2

Exercise 12.4.11 Factor $x^{375} + x^{250} + 2$ over $\mathbb{F}_5$ into the product of irreducibles.

Soln:

Observe that since $2 \in \mathbb{F}_5$, Frobenius automorphism fixes 2,

$$\mathbb{F}_5 \xrightarrow{\Phi} \mathbb{F}_5 \tag{1}$$

$$a \to a^5 \tag{2}$$

$$\text{where } \Phi(2) = 2^5 = 32 = 2 \mod 5. \tag{3}$$

Thus, $\Phi^3(2) = \Phi \circ \Phi \circ \Phi(2) = 2 \implies 2^{125} = 2$.
Thus, because *char* $\mathbb{F}_5 = 5$, we have

$$X^{375} + X^{250} + 2 = X^{375} + X^{250} + 2^{125} \tag{4}$$

$$= (X^3 + X^2 + 2)^{125} \tag{5}$$

If $X^3 + X^2 + 2$ is reducible in $\mathbb{F}_5$, it must have a linear factor, so suffice to check for linear factors.

$$\text{when } x = 0,\ x^3 + x^2 + 2 = 2 \tag{6}$$

$$\text{when } x = 1,\ x^3 + x^2 + 2 = 4 \tag{7}$$

$$\text{when } x = 2,\ x^3 + x^2 + 2 = 14 \tag{8}$$

$$\text{when } x = 3 = -2,\ x^3 + x^2 + 2 = 3 \tag{9}$$

$$\text{when } x = -1,\ x^3 + x^2 + 2 = 2 \tag{10}$$

Thus, $x^3 + x^2 + 2$ has no linear factors, hence irreducible.
So $(x^3 + x^2 + 2)^{125}$ is the desired factorization.

Problem 3

Exercise 13.3.3 Let $p \in \mathbb{Q}[x]$ be a quartic polynomial with $Gal_{\mathbb{Q}}(p) \cong D_4$, the dihedral group of order 8.

1. Show that p is irreducible over $\mathbb{Q}$.
2. Show that the cubic resolvent of p has a rational root.

Part A

Soln 1:
Let $p \in \mathbb{Q}[x]$ be quartic satisfying the assumption. Assume for contradiction that p is reducible.
So p factor into

1. $4 = 3 + 1$,
2. $4 = 2 + 2$,
3. $4 = 2 + 1 + 1$,
4. $4 = 1 + 1 + 1 + 1$

Case 1: $3+1$. a irred. cubic factor f and a linear factor. Then p has a root in $\mathbb{Q}$, and $Gal_{\mathbb{Q}}(p) = Gal_{\mathbb{Q}}(f)$, and since degree of extension of the splitting field of a polynomial of degree n is $\leq n!$, we have

$$|Gal_{\mathbb{Q}}(p)| = |Gal_{\mathbb{Q}}(f)| \leq 3! = 6, \tag{11}$$

$$\text{but } |Gal_{\mathbb{Q}}(p)| = 8. \tag{12}$$

Hence we have a contradiction.
Case 2: $2+2$. p factor into 2 quadratic factor, f and g. Now, let L be the splitting field of $f \cdot g$ over $\mathbb{Q}$. Then $|Gal_{\mathbb{Q}}(p)| = |[L : \mathbb{Q}]| \leq 4$. Reason: when we add the roots of f, we get a degree 2 extension (degree 2 extension is normal). Then if roots of g are already in this extension, $[L : \mathbb{Q}] = 2$, if not, then $[L : \mathbb{Q}] = 4$.
Case 3: $2 + 1 + 1$ we have $|Gal_{\mathbb{Q}}(p)| = 2$ Contradiction.
Case 4: $1 + 1 + 1 + 1$ we have $|Gal_{\mathbb{Q}}(p)| = 1$ Contradiction.

Part B

Soln 2:

$$\varphi : Gal_{\mathbb{Q}}(p) \hookrightarrow S_4 \tag{13}$$

We could imbed $Gal_{\mathbb{Q}}(p)$ into S_4 since an automorphism $\phi \in Gal_{\mathbb{Q}}(p)$ permutes the roots of p, (p is irred.) which we call $\alpha_1, \alpha_2, \alpha_3, \alpha_4$.
Thus, ϕ permutes the label $1, 2, 3, 4$. Since every element of $Gal_{\mathbb{Q}}(p)$ defines uniquely a permutation of $1, 2, 3, 4$, we could map $\phi \in Gal_{\mathbb{Q}}(p)$ to its corresponding permutation, which is a homomorphism, because both group operations are composition. This homomorphism φ is injective, since each element of $Gal_{\mathbb{Q}}(p)$ corresponds uniquely to a permutation. Thus,

$$D_4 \cong Gal_{\mathbb{Q}}(p) \cong Im\varphi \leq S_4 \tag{14}$$

Since groups of order 8 in S_4 are Sylow-2 subgroups of S_4, and they are all conjugates of each other, then any conjugate copy of $Im\varphi$ is going to act like D_4 on $\alpha_1, \alpha_2, \alpha_3, \alpha_4$, up to a relabel of the roots.
Thus, knowing $Gal_{\mathbb{Q}}(p) \cong D_4$ means $Gal_{\mathbb{Q}}(p)$ will act on the α's just like D_4 permutes $1, 2, 3, 4$, up to a

relabeling of the roots.
Thus, use the formula, let the roots of cubic resolvent of p be denoted by $\beta_1, \beta_2, \beta_3$, where

$$\beta_1 = (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4) \tag{15}$$
$$\beta_2 = (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4) \tag{16}$$
$$\beta_3 = (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3) \tag{17}$$

Write

$$D_4 = \{id, (1324), (12)(34), (1423), (13)(24), (14)(23), (12), (34)\} \tag{18}$$

Then we check

$$\beta_1^{id} = \beta_1 = (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4) \tag{19}$$
$$\beta_1^{(1324)} = (\alpha_3 + \alpha_4)(\alpha_2 + \alpha_1) = \beta_1 \tag{20}$$
$$\beta_1^{(12)(34)} = (\alpha_2 + \alpha_1)(\alpha_4 + \alpha_3) = \beta_1 \tag{21}$$
$$\beta_1^{(1423)} = (\alpha_4 + \alpha_3)(\alpha_1 + \alpha_2) = \beta_1 \tag{22}$$
$$\beta_1^{(12)} = (\alpha_2 + \alpha_1)(\alpha_3 + \alpha_4) = \beta_1 \tag{23}$$
$$\ldots \tag{24}$$

We could go on and check the action of all 8 elements of D_4. However, it would be sufficient to check that β_1 is fixed by the generators (1324) and (12).
Thus, β_1 is fixed by $Gal_{\mathbb{Q}}(p) \Rightarrow \beta_1 \in \mathbb{Q}$
Since the labeling of the roots $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ is arbitrary, we showed there is a rational root (of the cubic resolvent of p).

Problem 4

Exercise 13.3.5 Let α be a root of x^2+ax+b and β a root of x^3+px+q. Write down a polynomial with coefficients in $\mathbb{Q}(a,b,p,q)$ having $\alpha+\beta$ as a root.

Soln:

Let α_1, α_2 be roots of x^2+ax+b.
Let $\beta_1, \beta_2, \beta_3$ be roots of x^3+px+q. Hence,

$$\alpha_1+\alpha_2 = -a \tag{25}$$
$$\alpha_1 \cdot \alpha_2 = b \tag{26}$$

We have

$$\alpha_1^2+\alpha_2^2 = (\alpha_1+\alpha_2)^2 - 2\alpha_1\alpha_2 = a^2-2b \tag{27}$$
$$\alpha_1^3+\alpha_2^3 = (\alpha_1+\alpha_2)^3 - 3\alpha_1\alpha_2(\alpha_2+\alpha_1) = -a^3+3ba \tag{28}$$

Similarly, we have

$$\beta_1+\beta_2+\beta_3 = 0 \tag{29}$$
$$\beta_1\beta_2+\beta_1\beta_3+\beta_2\beta_3 = p \tag{30}$$
$$\beta_1\beta_2\beta_3 = -q \tag{31}$$

A polynomial with coefficients in $\mathbb{Q}(a,b,p,q)$ having $\alpha_i+\beta_j$ as a root is:

$$\prod_{i=1,j=1}^{2,3} (X-\alpha_i-\beta_j) \tag{32}$$

To see why this works, we expand:

$$\prod_{i=1,j=1}^{2,3} (X-\alpha_i-\beta_j) \tag{33}$$
$$= \big[(X-\alpha_1)^3 - \beta_3(X-\alpha_1)^2 - (\beta_1+\beta_2)(X-\alpha_1)^2 + (\beta_1+\beta_2)\beta_3(X-\alpha_1) + \beta_1\beta_2(X-\alpha_1) - \beta_1\beta_2\beta_3\big] \tag{34}$$
$$\cdot [\dots] \tag{35}$$
$$= \big[(X-\alpha_1)^3 + p(X-\alpha_1) + q\big]\big((X-\alpha_2)^3 + p(X-\alpha_2)+q\big) \tag{36}$$
$$= [X^2+aX+b]^3 + p^2[X^2+aX+b] + q^2 \tag{37}$$
$$+ p(X-\alpha_2)(X-\alpha_1)^3 + p(X-\alpha_1)(X-\alpha_2)^3 \tag{38}$$
$$+ q(X-\alpha_1)^3 + pq(X-\alpha_1) + q(X-\alpha_2)^3 + pq(X-\alpha_2) \tag{39}$$

expand, we have

$$= [X^2+aX+b]^3 + p^2[X^2+aX+b] + q^2 \tag{40}$$
$$+ p(X^2+aX+b)(X^2-2\alpha_1X+\alpha_1^2+X^2-2\alpha_2X+\alpha_2^2) \tag{41}$$
$$+ 2pqX + apqX \tag{42}$$
$$+ q[2X^3+3X(\alpha_1^2+\alpha_2^2)+3aX^2-(\alpha_1^3+\alpha_2^3)] \tag{43}$$

Now, use the expression for $\alpha_1+\alpha_2$, $\alpha_1^2+\alpha_2^2$, and $\alpha_1^3+\alpha_2^3$ that we obtained earlier, we see that we obtain a degree 6 polynomial with coefficients in $\mathbb{Q}(a,b,p,q)$. And we are done.