Galois Theory: GAL #08

Due on Apr 22, 2022 at 11:59pm

Prof Matyas Domokos Section 12

Xianzhi

2023

HW08
Apr 29, 2022
Exercise 12.4.8
Exercise 12.4.9
Exercise 12.4.10

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:

$\mathbb{F}_4 = \mathbb{F}_{2^2} = \mathbb{F}_2(\alpha)$ where α is a root of the irreducible polynomial $X^2 + X + 1$. Thus, $\alpha^2 + \alpha + 1 = 0$, so $\alpha^2 = \alpha + 1$. Hence,

$$\mathbb{F}_2(\alpha) = \{0, 1, \alpha, \alpha + 1\} \tag{1}$$

We want to factor $X^4 + X + 1 \in \mathbb{F}_2[X]$. First, we check if it has roots in $\mathbb{F}_2(\alpha)$:

$$X = 1 \implies X^4 + X + 1 = 1 \tag{2}$$
$$X = 0 \implies X^4 + X + 1 = 1 \tag{3}$$
$$X = \alpha \implies X^4 + X + 1 = (\alpha + 1)^2 + \alpha + 1 = \alpha^2 + 1 + \alpha + 1 = \alpha + 1 + \alpha = 1 \tag{4}$$
$$X = \alpha + 1 \implies (\alpha + 1)^4 + \alpha + 1 + 1 = (\alpha^2 + 1)^2 + \alpha = \alpha^2 + \alpha = 1 \tag{5}$$

so $X^4 + X + 1$ does not have linear factors in $\mathbb{F}_2(\alpha)$, so $X^4 + X + 1$ can only factor into

$$(X^2 + \alpha_1 X + \alpha_0)(X^2 + \beta_1 X + \beta_0) \tag{6}$$

for $\alpha_1, \alpha_0, \beta_1, \beta_0 \in \mathbb{F}_2(\alpha)$. Thus,

$$X^4 + X + 1 = X^4 + (\beta_1 + \alpha_1)X^3 + (\alpha_0 + \beta_0 + \alpha_1\beta_1)X^2 + (\alpha_1\beta_0 + \alpha_0\beta_1)X + \alpha_0\beta_0 \tag{7}$$

Hence,

$$\beta_1 + \alpha_1 = 0 \tag{8}$$
$$\alpha_0 + \beta_0 + \alpha_1\beta_1 = 0 \tag{9}$$
$$\alpha_1\beta_0 + \alpha_0\beta_1 = 1 \tag{10}$$
$$\alpha_0\beta_0 = 1 \tag{11}$$

implies

$$\alpha_1 = 1 \tag{12}$$
$$\beta_1 = 1 \tag{13}$$
$$\alpha_0 = \alpha \tag{14}$$
$$\beta_0 = \alpha + 1 \tag{15}$$

is one possible factorization. Hence,

$$X^4 + X + 1 = (X^2 + X + \alpha)(X^2 + X + \alpha + 1) \tag{16}$$

Now, in $\mathbb{F}_2(\alpha)$, degree 1 irreducible polynomials are

$$X, X + 1, X + \alpha, X + \alpha + 1 \tag{17}$$

degree 2 NOT irreducible:

$$X^2 + X, X^2 + \alpha X, X^2 + (\alpha + 1)X \tag{18}$$
$$X^2 + (\alpha + 1)X + \alpha, X^2 + (\alpha + 1)X + X + \alpha + 1 = X^2 + \alpha X + \alpha + 1 \tag{19}$$
$$X^2 + \alpha X + (\alpha + 1)X + 1 = X^2 + X + 1 \tag{20}$$

In $F_2(\alpha)$, we listed all 6 reducible polynomial of degree 2, since

$$X^2 + X + \alpha,\ X^2 + X + \alpha + 1 \tag{21}$$

are not among them, we know they must be irreducible. Hence, $X^4 + X + 1$ factors as product of irreducible over $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$.

$\mathbb{F}_4 = \mathbb{F}_{2^2} = \mathbb{F}_2(\alpha)$ *Why?* Since α is root of degree 2 irreducible polynomial, adjoining α to $\mathbb{F}_2$ gives degree 2 extension, since $\mathbb{F}_2(\alpha) : \mathbb{F}_2 = 2$, $\mathbb{F}_2(\alpha)$ has 4 elements, and since the finite field of a prime power (4 in this case) is unique, we indeed get $\mathbb{F}_4$ by adjoin α to $\mathbb{F}_2$.

Problem 2

Exercise 12.4.9

1. What is the splitting field of $X^4 + X + 1$ over $\mathbb{F}_{64}$?
2. Factor $X^4 + X + 1$ into the product of irreducibles over $\mathbb{F}_{64}$.

Soln:
Part A

Let β be root of $X^4 + X + 1$ over $\mathbb{F}_2$.
Let α be root of $X^6 + X + 1$ over $\mathbb{F}_2$.

$$\mathbb{F}_2 \subseteq \mathbb{F}_{16} = \mathbb{F}_2(\beta) \subseteq \mathbb{F}_{2^{12}} = \mathbb{F}_2(\alpha, \beta) \tag{22}$$

$$\mathbb{F}_2 \subseteq \mathbb{F}_{64} = \mathbb{F}_2(\alpha) \subseteq \mathbb{F}_{2^{12}} = \mathbb{F}_2(\alpha, \beta). \tag{23}$$

In class we established that $X^6 + X + 1$ is irreducible over $\mathbb{F}_2$, so let α be a root of $X^6 + X + 1$ over $\mathbb{F}_2$. Then $\mathbb{F}_{64} = \mathbb{F}_2(\alpha)$ since adjoining α gives a degree 6 extension over $\mathbb{F}_2$, and there is only one field of 2^6 elements up to isomorphism, so $\mathbb{F}_2(\alpha)$ is indeed $\mathbb{F}_{64}$.
We also established that $X^4 + X + 1$ is irreducible over $\mathbb{F}_2$, and since finite extension of finite field is Galois, it is normal, so adding one root β of $X^4 + X + 1$ to $\mathbb{F}_2$ automatically adds all the roots. Thus, the splitting field of X^4+X+1 over $\mathbb{F}_2$ is $\mathbb{F}_2(\beta) = \mathbb{F}_{2^4}$ again because $\exists!$ field of 16 elements (up to isomorphism).

The splitting field of $X^4 + X + 1$ over $\mathbb{F}_{64}$ must contain $\mathbb{F}_2(\alpha) = \mathbb{F}_{64}$ and β so the splitting field is $\mathbb{F}_2(\alpha, \beta)$, (since adding one root automatically adds all other roots of $X^4 + X + 1$.) Since

$$\mathbb{F}_{p^r} \subseteq \mathbb{F}_{p^s} \iff r \mid s \tag{24}$$

$$lcm(4, 6) = 12, \tag{25}$$

$\mathbb{F}_{2^{12}}$ is the smallest field containing both $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^6}$.
So $\mathbb{F}_{2^{12}} = \mathbb{F}_2(\alpha, \beta)$ is the splitting field of $X^4 + X + 1$ over $\mathbb{F}_{2^6}$.

Part B

Claim: $X^4 + X + 1$ cannot have any root in $\mathbb{F}_{64}$.
Assume $X^4 + X + 1$ has a root in $\mathbb{F}_{64}$, Then $\mathbb{F}_{64}$ contains all the roots of $X^4 + X + 1$. Thus, $\mathbb{F}_64$ is itself the splitting field of $X^4 + X + 1$ over $\mathbb{F}_{64}$, which is a contradiction.

Thus, $X^4 + X + 1$ does not have linear factors in $\mathbb{F}_{64}$, so factorization $3 + 1$ and $1 + 1 + 2$ cannot happen. Also, since splitting field of $X^4 + X + 1$, $\mathbb{F}_{2^{12}}$, is degree 2 extension over $\mathbb{F}_{2^6}$, we deduce that the only way to factor $X^4 + X + 1$ into irred. factors over $\mathbb{F}_{64}$ is

$$(X^2 + a_1X + a_0)(X^2 + b_1X + b_0) \tag{26}$$

In perticular, $X^4 + X + 1$ must be reducible over $\mathbb{F}_{64}$.
since $\mathbb{F}_{2^2} \subseteq \mathbb{F}_{2^6}$ because $2 \mid 6$,
the same factorization in **12.4.8** works here.

$$X^4 + X + 1 = (X^2 + X + \alpha)(X^2 + X + \alpha + 1) \tag{27}$$

for $\alpha^2 = \alpha + 1$, where α is a root of irred. polynomial $X^2 + X + 1$ over $\mathbb{F}_2$.
If we let $\mathbb{F}_{2^6}$ be $\mathbb{F}_2(\gamma)$ where γ is a root of irred. polynomial $X^6 + X + 1$ over $\mathbb{F}_2$, we should be able to identify α with an element in $\mathbb{F}_2(\gamma)$ of the form

$$a_5\gamma^5 + a_4\gamma^4 + \ldots + a_1\gamma + a_0 \tag{28}$$

Problem 2 continued on next page...

where $a_i = 0$ or 1, since $\mathbb{F}_4 \subseteq \mathbb{F}_{64}$.

Since $\mathbb{F}_{64}^{\times}$ has 63 elements, and $\mathbb{F}_2(\alpha) = \mathbb{F}_4$, where α is root of $X^2 + X + 1$, we deduce α is a primitive 3rd root of unity, so if $\mathbb{F}_{64} = \mathbb{F}_2(\gamma)$ where γ is root of irreducible polynomial $X^6 + X + 1$, we have

$$\alpha \leftrightarrow \gamma^{21} \tag{29}$$
$$\alpha^2 = \alpha + 1 \leftrightarrow \gamma^{42} \tag{30}$$
$$\alpha^3 = (\alpha + 1)\alpha = \alpha^2 + \alpha = 1 \leftrightarrow \gamma^{63} = 1 \tag{31}$$
$$\text{thus, } X^4 + X + 1 = (X^2 + X + \gamma^{21})(X^2 + X + \gamma^{42}) \tag{32}$$

in $\mathbb{F}_2(\gamma) = \mathbb{F}_{64}$.
We double check: RHS of equation (32) is

$$X^4 + (\gamma^{42} + \gamma^{21} + 1)X^2 + (\gamma^{42} + \gamma^{21})X + 1 \tag{33}$$

Since $\gamma^6 = \gamma + 1$, we have

$$\gamma^{21} = (\gamma^6)^3 \cdot \gamma^3 = (\gamma + 1)^3 \cdot \gamma^3 = (\gamma^2 + 1)(\gamma + 1)\gamma^3 = \gamma + 1 + \gamma^5 + \gamma^4 + \gamma^3 \tag{34}$$

Similarly, we have

$$\gamma^{42} = (\gamma + 1)^7 = (\gamma^2 + 1)^3(\gamma + 1) = (\gamma^6 + 1 + 3\gamma^4 + 3\gamma^2)(\gamma + 1) = (\gamma + 3\gamma^4 + 3\gamma^2)(\gamma + 1) = \gamma^5 + \gamma^4 + \gamma^3 + \gamma \tag{35}$$

Hence, we have

$$\gamma^{42} + \gamma^{21} = 1 \tag{36}$$
$$\gamma^{42} + \gamma^{21} + 1 = 0 \tag{37}$$

as wanted.

Problem 3

Exercise 12.4.10

1. Show that the polynomial $X^2 + 1$ is irreducible over $\mathbb{F}_7$.
2. Consider the field $\mathbb{F}_7(\alpha)$, where α is a root of $X^2 + 1$. Show that all quadratic polynomials over $\mathbb{F}_7$ have a root in $\mathbb{F}_7(\alpha)$.
3. Determine explicitly the roots in $\mathbb{F}_7(\alpha)$ of $5X^2 + 3X + 1 \in \mathbb{F}_7[X]$.

Soln:
Part A

o show $X^2 + 1$ is irreducible over $\mathbb{F}_7$, we show $X^2 + 1$ does not factor into linear factors which is equivalent to show $X^2 + 1$ does not have root in $\mathbb{F}_7$.

$$X = 0 \to X^2 + 1 = 1 \tag{38}$$
$$X = 1 \to X^2 + 1 = 2 \tag{39}$$
$$X = 2 \to X^2 + 1 = 5 \tag{40}$$
$$X = 3 \to X^2 + 1 = 3 \mod 7 \tag{41}$$
$$X = 4 \to X^2 + 1 = 3 \mod 7 \tag{42}$$
$$X = 5 \to X^2 + 1 = 5 \mod 7 \tag{43}$$
$$X = 6 \to X^2 + 1 = 2 \mod 7 \tag{44}$$

None of them is zero, so $X^2 + 1$ does not have root in $\mathbb{F}_7$, so $X^2 + 1$ is irreducible over $\mathbb{F}_7$.

Part B

irst, assume quadratic polynomial f is not irreducible. Thus, f can be factored into 2 linear factors, $\implies$ the roots of f are in $\mathbb{F}_7$, and $\mathbb{F}_7$ is certainly contained in $\mathbb{F}_7(\alpha)$.
Now, assume f is irred. Let β be a root of f. Since f is quadratic, $\mathbb{F}_7(\beta)$ is degree 2 extension of $\mathbb{F}_7$, (which is also normal, since finite extensions of finite fields are Galois.) Thus, $\mathbb{F}_7(\beta)$ contains all roots of f. Since

$$\mathbb{F}_7 \subseteq \mathbb{F}_7(\alpha) \subseteq L \tag{45}$$
$$\mathbb{F}_7 \subseteq \mathbb{F}_7(\beta) \subseteq L \tag{46}$$

where L is the algebraic closure of $\mathbb{F}_7$. Then $\mathbb{F}_7(\alpha)$ and $\mathbb{F}_7(\beta)$ are the same field, since the finite field of any prime power order is unique.

Part C

etermine roots in $\mathbb{F}_7(\alpha)$ of $5X^2 + 3X + 1 \in \mathbb{F}_7[X]$ Let $a, b \in \mathbb{F}_7$, remember $\alpha^2 + 1 = 0$. $\mathbb{F}_7(\alpha)$ is degree 2 vector space over $\mathbb{F}_7$, so a general element is of the form $a\alpha + b$.

$$5(a\alpha + b)^2 + 3(a\alpha + b) + 1 = 0 \tag{47}$$
$$5(a^2\alpha^2 + 2ab\alpha + b^2) + 3a\alpha + 3b + 1 = 0 \tag{48}$$
$$5a^2(-1) + 10ab\alpha + 5b^2 + 3a\alpha + 3b + 1 = 0 \tag{49}$$
$$2a^2 + 3ab\alpha + 5b^2 + 3a\alpha + 3b + 1 = 0 \tag{50}$$
$$\tag{51}$$

Thus,

$$3ab + 3a = 0 \tag{52}$$
$$2a^2 + 5b^2 + 3b + 1 = 0 \tag{53}$$

Hence, we have case (1)

$$a = 0 \tag{54}$$
$$5b^2 + 3b + 1 = 0 \tag{55}$$

OR case (2)

$$b = -1 \tag{56}$$
$$2a^2 + 5 - 3 + 1 = 0 \tag{57}$$

If case (1), then we could stop because $5X^2 + 3X + 1$ has no roots in $\mathbb{F}_7$.

$$
\begin{aligned}
X = 1 &\to 5X^2 + 3X + 1 = 2 && (58)\\
X = 2 &\to 5X^2 + 3X + 1 = 6 && (59)\\
X = 3 &\to 5X^2 + 3X + 1 = 6 \mod 7 && (60)\\
X = 4 &\to 5X^2 + 3X + 1 = 2 \mod 7 && (61)\\
X = 5 &\to 5X^2 + 3X + 1 = 1 \mod 7 && (62)\\
X = 6 &\to 5X^2 + 3X + 1 = 3 \mod 7 && (63)\\
& && (64)
\end{aligned}
$$

so no roots in $\mathbb{F}_7$.
In case (2), we have

$$
\begin{gathered}
b = -1\\
2a^2 = -3\\
\text{which implies}\\
b = 6\\
2a^2 = 4
\end{gathered}
$$

Hence, we have $b = 6,\ a = 3$ (since $18 \equiv 4$) or $b = 6,\ a = 4$ (since $32 \equiv 4 \mod 7$).
Thus, the roots are $3\alpha + 6$ and $4\alpha + 6$.
We could double check

$$
\begin{aligned}
5(X - 6 - 3\alpha)(X - 6 - 4\alpha) &= 5(X^2 - 12X + 36 + 12\alpha^2 - 7\alpha(X - 6)) && (65)\\
&= 5(X^2 + 2X + 1 - 5) && (66)\\
&= 5X^2 + 3X + 1 \mod 7. && (67)
\end{aligned}
$$