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

# 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:

# 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 $\alpha$ 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: