Galois Theory: GAL #10

Due on May 6, 2022 at 11:59pm

Prof Matyas Domokos Section 12 & 15

Xianzhi

2023

HW10
Exercise 12.4.12
Exercise 12.4.13
Exercise 15.1.2

Problem 1

Exercise 12.4.12 Prove that $X^4 - 10X^2 + 1$ is irreducible over $\mathbb{Q}$, but it is reducible in $(\mathbb{Z}/p\mathbb{Z})[X]$ for any prime p.

Soln:

Part A

Proof. We claim the minimum polynomial is $M_{\mathbb{Q}}(\sqrt{2}+\sqrt{3}) = X^4 - 10X^2 + 1$. Observe that

$$
\begin{aligned}
&(\sqrt{2}+\sqrt{3})^4 - 10(\sqrt{2}+\sqrt{3})^2 + 1 && (1)\\
=&(5+2\sqrt{6})^2 - 10(5+2\sqrt{6}) + 1 && (2)\\
=&0 && (3)
\end{aligned}
$$

Thus, $(\sqrt{2}+\sqrt{3})$ is a root of $X^4 - 10X^2 + 1$. Claim: $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, and it is a degree 4 extension over $\mathbb{Q}$, so $X^4 - 10X^2 + 1$ is the minimal polynomial over $\mathbb{Q}$, hence irreducible.
Now we show the claim. $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \supset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ because

$$
\begin{aligned}
5+2\sqrt{6} = (\sqrt{2}+\sqrt{3})^2 &\in \mathbb{Q}(\sqrt{2}+\sqrt{3}) && (4)\\
\implies \sqrt{6}(\sqrt{2}+\sqrt{3}) &\in \mathbb{Q}(\sqrt{2}+\sqrt{3}) && (5)\\
\implies \sqrt{2} = \sqrt{6}(\sqrt{2}+\sqrt{3}) - 2(\sqrt{2}+\sqrt{3}) &\in \mathbb{Q}(\sqrt{2}+\sqrt{3}) && (6)\\
\implies \sqrt{3} = \sqrt{2}+\sqrt{3}-\sqrt{2} &\in \mathbb{Q}(\sqrt{2}+\sqrt{3}) && (7)\\
& && (8)
\end{aligned}
$$

$\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ because $\sqrt{2}+\sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Hence, we showed $X^4 - 10X^2 + 1$ is irreducible over $\mathbb{Q}$.

□

Part B

Proof. Now, observe

$$
\begin{aligned}
X^4 - 10X^2 + 1 &= (X^2-5)^2 - 2^2 \cdot 6 && (9)\\
&= (X^2-1)^2 - (2X)^2 \cdot 2 && (10)\\
&= (X^2+1)^2 - (2X)^2 \cdot 3 && (11)
\end{aligned}
$$

Thus, in $(\mathbb{Z}/p\mathbb{Z})$, as long as at least one of $6, 2, 3$ is a square, then $X^4 - 10X^2 + 1$ factors in $\mathbb{Z}/p\mathbb{Z}[X]$ use formula $a^2 - b^2 = (a+b)(a-b)$.
For any prime p, $\mathbb{Z}/p\mathbb{Z}^\times = \mathbb{F}_p^\times = \mathbb{F}_p \setminus \{0\}$ is cyclic, (multiplicative group of any finite field is cyclic), $\exists$ generator g, thus

$$\{1, g, g^2, g^3, g^4, \cdots, g^{p-2}\} = \mathbb{F}_p^\times \tag{12}$$

Those with even power are squares.
Assume for contradiction that all $2, 3, 6$ are not squares in $\mathbb{F}_p$.
$\implies \; 2 = g^j, \; 3 = g^i$ for some j, i odd.
But $6 = g^{j+i}$ has even power $j+i$, so 6 should be square in $\mathbb{F}_p$. We have a contradiction.
Thus, $\exists$ at least 1 square among $2, 3, 6$. And we are done. □

Problem 2

Exercise 12.4.13 Let K be a field of characteristic p (where p is a prime), and suppose that $f = X^p - X - a \in K[X]$ is irreducible. Show that f is separable, and determine the Galois group of f. *Warning: K is not assumed to be finite.)*

Soln:

Proof. □

Problem 3

Exercise 15.1.2 Let p be a prime and n a positive integer. For $d \in \mathbb{N}$ denote by $\overline{\Phi}_d \in (\mathbb{Z}/p\mathbb{Z})[X]$ the modulo p reduction of the cyclotomic polynomial $\Phi_d \in \mathbb{Z}[X]$. Show that the splitting field of $\overline{\Phi}_{p^n-1}$ over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is the field $\mathbb{F}_{p^n}$.

Soln: