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. Let α be a root of $f = X^p - X - a \in K[X]$.
Claim: the p roots of f are $\alpha + \beta$ for $\beta \in \mathbb{F}_p = \{0, 1, \cdots, p-1\}$. We have $\alpha^p - \alpha - a = 0$. Let $\beta \in \mathbb{F}_p$.

$$\begin{aligned}
&(\alpha+\beta)^p - (\alpha+\beta) - a && (13)\\
=&\alpha^p + \beta^p - \alpha - \beta - a \text{ because } charK = p && (14)\\
=&\beta^p - \beta \mod p && (15)\\
=&0 && (16)
\end{aligned}$$

where the last step is due to Fermat's little theorem, which states, for integer z, prime p, we have

$$z^p = z \mod p.$$

Thus, $\alpha + \beta$ is a root of f.
Since f has p roots, letting $\beta \in \mathbb{F}_p$ gives exactly the p roots $\alpha+0, \alpha+1, \cdots, \alpha+p-1$, and they are distinct. Thus, f is separable. $Gal_k(f) = \Gamma(L : K)$ where L is the splitting field of f over K. We see that $L = K(\alpha)$ for a root α of f, since once we adjoin α, other roots can be obtained by $\alpha + \beta$, with $\beta \in \mathbb{F}_p \subset K$.
(K certainly contains it's prime subfield that is isomorphic to $\mathbb{F}_p$.) Since f is irreducible,

$$|\Gamma(L : K)| = |[L : K]| = |[K(\alpha) : K]| = p \tag{17}$$

and this extension is Galois because it is a splitting field of a separable polynomial.
Thus, $\Gamma(L : K)$ is cyclic. All groups of prime order are cyclic. □

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:

We have

$$\prod_{d|p^n-1} \Phi_d = X^{p^n-1} - 1 \tag{18}$$

reduce modulo p, we get

$$\prod_{d|p^n-1} \overline{\Phi}_d = X^{p^n-1} - 1 \tag{19}$$

Let L be the splitting field of $\overline{\Phi}_{p^n-1}$ over $\mathbb{F}_p$.
Then $L \subset \mathbb{F}_{p^n}$, since roots of $\overline{\Phi}_{p^n-1}$ are roots of $X^{p^n-1} - 1$ and roots of $X^{p^n-1} - 1$ are precisely the elements of $\mathbb{F}_{p^n}^\times$. ($\implies$ roots of $\overline{\Phi}_{p^n-1} \subset \mathbb{F}_{p^n}^\times$).
To show $L \supset \mathbb{F}_{p^n}$, we want the generators of $\mathbb{F}_{p^n}^\times$ as a cyclic group to be roots of $\overline{\Phi}_{p^n-1}$. We show any generator g of $\mathbb{F}_{p^n}^\times$ cannot be a root of $\overline{\Phi}_d$ where $d < p^n - 1$. For $d < p^n - 1$, we have

$$\prod_{e|d} \Phi_e = X^d - 1 \tag{20}$$

reduce mod p,

$$\prod_{e|d} \overline{\Phi}_e = X^d - 1 \tag{21}$$

Then any root α of $\overline{\Phi}_d$ is also a root of $X^d - 1$, so $\alpha^d = 1$, which implies $|\alpha|$ divide d, which implies $|\alpha| \leq d$.
Hence, roots of $\overline{\Phi}_d$ with $d < p^n - 1$ has order $\leq d < p^n - 1$,
so, roots of $\overline{\Phi}_d$ with $d < p^n - 1$ cannot be generators.
Since generators of $\mathbb{F}_{p^n}^\times$ are roots of $X^{p^n-1} - 1$, so they are roots of

$$\prod_{d|p^n-1} \overline{\Phi}_d, \tag{22}$$

and they have order $= p^n - 1$, so they can only be roots of $\overline{\Phi}_{p^n-1}$.
Thus, the splitting field of $\overline{\Phi}_{p^n-1}$, L over $\mathbb{F}_p$ contains the generators of $\mathbb{F}_{p^n}^\times$, thus, $L \supset \mathbb{F}_{p^n}$.
Thus, $L = \mathbb{F}_{p^n}$.