Math 505 HW4

Rohan Mukherjee

February 7, 2024

Problem 1.

(1) We showed on HW1 (and HW3) that $f(x) = x^{p-1} + \cdots + 1$ is irreducible. Since $\mathbb{Q}$ has characteristic 0 any irreducible polynomial is separable, so we only need to show that $\mathbb{Q}(\rho)/\mathbb{Q}$ is normal. This follows immediately as,

$$f(x) = \prod_{n=1}^{p-1}(x - \rho^n)$$

As was shown on HW1, so $\mathbb{Q}(\rho)$ is a splitting field and hence normal.

(2) We shall show that $\mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})$ is cyclic and has order $p-1$, thus is isomorphic to $(\mathbb{Z}/p)^{\times}$. First, notice that the claim is trivial for $p = 2$ since in that case the splitting field of $x + 1$ is just $\mathbb{Q}$, so let p be an odd prime. Let α be a generator for the cyclic group $(\mathbb{Z}/p)^{\times}$. We claim that $\mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})$ is generated by

$$\sigma : \mathbb{Q}(\rho) \to \mathbb{Q}(\rho)$$
$$\sigma : \rho \mapsto \rho^{\alpha}$$

Notice first that

$$\mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q}) = \{\, \sigma : \rho \mapsto \rho^n \mid n \in [p-1] \,\}$$

Since specifying where ρ goes completely determines the automorphism, and we have $p-1$ choices to send ρ to, being any root of $f(x) = x^{p-1} + \cdots + 1$. Let $n \in [p-1]$ be an integer. Since α is a generator of $(\mathbb{Z}/p)^{\times}$, we can find a k such that $\alpha^k = n$. Now, $\sigma^k(\rho) = \rho^{\alpha^k} = \rho^n$, which completes the proof. The obvious isomorphism is just $\alpha \mapsto \sigma : \rho \mapsto \rho^{\alpha}$.

Problem 2.

Let $f(x) = x^p - 2$ and ζ be a primitive pth root of unity. We see immediately that $\left\{ \sqrt[p]{2}, \sqrt[p]{2}\zeta, \ldots, \sqrt[p]{2}\zeta^{p-1} \right\}$ are all the p distinct roots of this irreducible polynomial, so in particular,

$$\mathbb{Q}_f = \mathbb{Q}\left(\sqrt[p]{2}, \zeta\right)$$

We have the following diagram of field extensions:

$$\begin{tikzcd}[column sep=small]
 & \mathbb{Q}\left(\sqrt[p]{2}, \zeta\right) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}\left(\sqrt[p]{2}\right) \arrow[dr, dash, "p"'] & & \mathbb{Q}(\zeta) \arrow[dl, dash, "p-1"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Where the degrees marked are obvious (For example, $x^p - 2$ is irreducible, and we calculated the bottom-right extension in the last problem). Since $g(x) = x^{p-1} + \cdots + 1$ is a polynomial with ζ as a root, it follows that $|\mathbb{Q}\left(\sqrt[p]{2}, \zeta\right) : \mathbb{Q}(\sqrt[p]{2})| \leq p - 1$. Since p and $p-1$ are coprime, we have that $p(p-1) \mid |\mathbb{Q}\left(\sqrt[p]{2}, \zeta\right) : \mathbb{Q}|$, and also that

$$|\mathbb{Q}\left(\sqrt[p]{2}, \zeta\right) : \mathbb{Q}| = |\mathbb{Q}\left(\sqrt[p]{2}, \zeta\right) : \mathbb{Q}(\sqrt[p]{2})| \cdot |\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}| \leq (p-1)p$$

Thus $|\mathbb{Q}\left(\sqrt[p]{2}, \zeta\right) : \mathbb{Q}| = p(p-1)$. Once again let α be a generator for $(\mathbb{Z}/p)^\times$. Notice that,

$$\sigma : \begin{cases} \sqrt[p]{2} \mapsto \sqrt[p]{2}\zeta \\ \zeta \mapsto \zeta \end{cases} \qquad \text{has order } p$$

$$\tau : \begin{cases} \sqrt[p]{2} \mapsto \sqrt[p]{2} \\ \zeta \mapsto \zeta^\alpha \end{cases} \qquad \text{has order } p-1$$

Notice also that if G is a group of order $p(p-1)$, then $n_p \equiv 1 \mod p$ and $n_p \mid p-1$ so the subgroup of order p is normal, so if $H \leq G$ is the subgroup of order p, and if there is a subgroup N of order $p-1$, then $G \cong H \rtimes N$. Notice that $\tau\sigma\tau^{-1}(\sqrt[p]{2}) = \tau\sigma(\sqrt[p]{2}) = \tau(\sqrt[p]{2}\zeta) = \sqrt[p]{2}\zeta^\alpha$, and $\tau\sigma\tau^{-1}(\zeta) = \zeta$. Thus $\tau\sigma\tau^{-1} = \sigma^\alpha$.

Thus $\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt[p]{2}, \zeta\right)/\mathbb{Q}\right) \cong \langle\sigma\rangle \rtimes \langle\tau\rangle \cong \mathbb{Z}/p \rtimes (\mathbb{Z}/p)^\times$ with multiplication on the furthest right group given by $(a,b)(c,d) = (a+cb, bd)$. This is just the holomorph of $\mathbb{Z}/p$, i.e. $\mathrm{Gal}\Big(\mathbb{Q}\Big(\sqrt[p]{2},\zeta\Big)/\mathbb{Q}\Big) \cong \mathbb{Z}/p \rtimes \mathrm{Aut}(\mathbb{Z}/p) = \mathrm{Hol}(\mathbb{Z}/p)$.

Problem 3.

(1) We first prove the following lemma.

Lemma 1. *For coprime $a,b \in \mathbb{Z}$, (at least) one of which is not a perfect square, $\sqrt{\frac{a}{b}} \notin \mathbb{Q}$.*

Proof. Suppose that $d\sqrt{p} = c\sqrt{q}$ for $c,d \in \mathbb{Z}$ coprime neither of which are 0. Squaring both sides shows that $d^2b = c^2a$. WLOG let a be the non-perfect square, and p a prime divisor whose power in the prime factorization of a is not a multiple of 2. It follows that $p \mid d^2$ so $p \mid d$, so write $d = d'p$ and we see that $d'^2p^2b = c^2a$, equivalently $d^2pb = c^2\frac{a}{p}$. If $\frac{a}{p}$ is not divisible by p then $p \mid c^2$ so $p \mid c$ a contradiction, otherwise keep canceling factors of p from a until this happens. $\square$

We claim that $\mathbb{Q}(\sqrt{17},\sqrt{239})$ is a degree 4 Galois extension over $\mathbb{Q}$. If not, we would have $\mathbb{Q}(\sqrt{17},\sqrt{239}) = \mathbb{Q}(\sqrt{17}) = \mathbb{Q}(\sqrt{239})$. Then $\sqrt{239} = a\sqrt{17} + b$. Squaring both sides shows that $b = 0$ (otherwise $\sqrt{17}$ would be rational). This would say that $\sqrt{\frac{239}{17}} \in \mathbb{Q}$, which is false by the lemma. Notice that $|\mathbb{Q}(\sqrt{17},\sqrt{239}) : \mathbb{Q}| \leq 4$ since $x^2 - 239$ is a degree 2 polynomial with coefficients in $\mathbb{Q}(\sqrt{17})$ with $\sqrt{239}$ as a root. Thus $\mathbb{Q}(\sqrt{17},\sqrt{239}$ has degree strictly greater than 2, ≤ 4, and divisible by 2, so it equals 4. The extension is Galois as $\mathbb{Q}$ has characteristic 0 and it is the splitting field of $(x^2-17)(x^2-239)$. We now compute $\mathrm{Gal}\Big(\mathbb{Q}(\sqrt{17},\sqrt{239})/\mathbb{Q}\Big)$. $x^2 - 17$ is an irreducible polynomial with $\sqrt{17}$ as a root, thus $\sqrt{17}$ must get sent to either itself or the other root of this polynomial: $-\sqrt{17}$. $x^2 - \sqrt{239}$ is an irreducible polynomial with coefficients in $\mathbb{Q}(\sqrt{17})$ (It is irreducible by our lemma above–this field does not contain $\sqrt{239}$), so $\sqrt{239}$ goes to $\pm\sqrt{239}$. Thus the Galois group is generated by $\sigma : \sqrt{17} \mapsto -\sqrt{17}$ and $\tau : \sqrt{239} \mapsto -\sqrt{239}$, which are both of order 2, so the Galois group is equal to $\mathbb{Z}/2 \times \mathbb{Z}/2$. The four conjugates of $\sqrt{17} + \sqrt{239}$ under the action of the Galois group are

$$\pm\sqrt{17} \pm \sqrt{239}$$

In particular, the only element of the Galois group fixing $\sqrt{17} + \sqrt{239}$ is just e. Thus

$\mathbb{Q}(\sqrt{17}+\sqrt{239}) = \mathbb{Q}(\sqrt{17}, \sqrt{239})^{\langle e\rangle} = \mathbb{Q}(\sqrt{17}, \sqrt{239})$. Multiplying together

$$\begin{aligned}(x-(\sqrt{17}+\sqrt{239}))(x-(-\sqrt{17}+\sqrt{239}))(x-(\sqrt{17}-\sqrt{239}))(x-(-\sqrt{17}-\sqrt{239}))\\ = x^4 - 512x^2 + 49284\end{aligned}$$

Which is a monic degree 4 polynomial with $\sqrt{17}+\sqrt{239}$ as a root, and since the field extension $\mathbb{Q}(\sqrt{17}+\sqrt{239})$ has degree 4 this polynomial must be irreducible.

(2) Notice first that $\mathbb{Q}(1+\sqrt[3]{2}+\sqrt[3]{4}) = \mathbb{Q}(\sqrt[3]{2})$, since we have the forward inclusion and $1 < |\mathbb{Q}(1+\sqrt[3]{2}+\sqrt[3]{4}) : \mathbb{Q}| \leq 3$ (It cannot be 2 since its degree must divide 3). Now, we prove the following lemma.

Lemma 2. *Let F be an extension with a fixed algebraic closure $\overline{F}$, $\alpha, \beta \in \overline{F}$, $f = \mathrm{Irr}_F(\alpha)$, and $g = \mathrm{Irr}_F(\beta)$. If $F(\alpha) = F(\beta)$, then $F_f = F_g$.*

Proof. Let $|F(\alpha) : F| = |F(\beta) : F| = n$, and let $\alpha_2, \dots, \alpha_n$ be the rest of the roots (not necessarily distinct) of f, and $\beta_2, \dots, \beta_n$ be the rest of the roots of g. Since $F_f = F(\alpha, \alpha_2, \dots, \alpha_n)$ is normal containing β, it must contain $\beta_2, \dots, \beta_n$. The reverse inclusion is the same, which completes the proof. □

We need only complete the Galois group over the splitting field of $\mathbb{Q}(\sqrt[3]{2})$. But we have already done this in class–the splitting field is $\mathbb{Q}(\sqrt[3]{2}, \zeta)$, where ζ is a primitive 3rd root of unity, with Galois group $D_3 \cong S_3$. Now, recall that $\sigma : \sqrt[3]{2} \mapsto \sqrt[3]{2}\zeta$ was an automorphism of order 3. The powers of this automorphism will give us the conjugates of $1+\sqrt[3]{2}+\sqrt[3]{4}$. The other two conjugates are,

$$\begin{aligned}1+\sqrt[3]{2}\zeta+\sqrt[3]{4}\zeta^2\\ 1+\sqrt[3]{2}\zeta^2+\sqrt[3]{4}\zeta\end{aligned}$$

Thus the minimal polynomial is,

$$\begin{aligned}(x-(1+\sqrt[3]{2}+\sqrt[3]{4}))(x-(1+\sqrt[3]{2}\zeta+\sqrt[3]{4}\zeta^2))(x-(1+\sqrt[3]{2}\zeta^2+\sqrt[3]{4}\zeta))\\ = x^3 - 3x^2 - 3x - 1\end{aligned}$$

Notice once again that this is indeed the minimal polynomial since it has the minimal degree of 3.

Problem 4.

(1) A reduction of $X^3 - X - 1$ over $\mathbb{Q}$ would yield a reduction over $\mathbb{Z}$, which would yield an integer root of this polynomial. Then $X(X^2 - 1) = 1$ would have an integer solution. Thus we must have either $X = 1$ and $X^2 - 1 = 1$, or $X = -1$ and $X^2 - 1 = -1$. Both cases cannot be–for example, if $X = 1$ then $X^2 - 1 = 0 \neq 1$, so $X^3 - X - 1$ is irreducible over $\mathbb{Q}$. We recall the theorem from class that says the Galois group will be S_3 iff the discriminant is not a square. Recall that the formula for the discriminant of a polynomial $f(x) = x^3 + px + q$ is just $-4p^3 - 27q^2$. So, the discriminant of $f(x) = X^3 - X - 1$ is just $-4(-1)^3 - 27(-1)^2 = 4 - 27 = -23$, so the discriminant is not a square since $\mathbb{Q}$ does not contain any complex values. Thus, $\mathrm{Gal}\left(\mathbb{Q}_f\right) = S_3$.

(2) The roots of this polynomial over $\mathbb{C} = \overline{\mathbb{Q}}(\sqrt{2})$ are $\sqrt{10}$, $\sqrt{10}\zeta$, $\sqrt{10}\zeta^2$ where ζ is a primitive third root of unity. Clearly the last two are not in $\mathbb{Q}(\sqrt{2})$, and the first isn't, otherwise $\sqrt{5} \in \mathbb{Q}(\sqrt{2})$, and by similar reasoning from problem 1 part (1) this would say that $\sqrt{5/2}$ is a rational number, a contradiction. Thus $X^3 - 10$ is irreducible. Once again we find the discriminant to be $-4(0^3) - 27(10)^2 = -2700$. Again $\mathbb{Q}(\sqrt{2})$ does not contain any complex numbers, thus the discriminant is not a square, so the splitting field's Galois group will be S_3.

(3) Recall that a cubic polynomial is irreducible iff it splits into a linear and a quadratic factor. In particular, it must have a root. If $X^3 - X - t$ was reducible in $\mathbb{C}(t)$, since $\mathbb{C}[t]$ is a UFD, $X^3 - X - t$ would be reducible over $\mathbb{C}[t]$. Thus there would be a polynomial $p(t) \in \mathbb{C}[t]$ such that

$$p(t)^3 = p(t) - t$$

The degree of the LHS is $3 \deg p(t)$, and the degree of the RHS is $\leq \max \deg p(t), 1$. Thus we have that either $3 \deg p(t) \leq \deg p(t)$ thus $\deg p(t) = 0$, or $3 \deg p(t) \leq 1$ thus $\deg p(t) = 0$. In any case $p(t) \equiv c \in \mathbb{C}$. This would claim that $c^3 = c - t$, but the degree of the RHS is 1 while the LHS is 0, a contradiction.

We calculate the discriminant to be $-4(-1)^3 - 27(-t)^2 = 4 - 27t^2$. This is a square iff $f(X) = X^2 - 4 + 27t^2$ has a root in $\mathbb{C}(t)$. Suppose instead that

$$a + bt^2 = \left(\frac{p(t)}{q(t)}\right)^2$$

With $p(t), q(t) \in \mathbb{C}[t]$. The equation $q(t)^2(a + bt^2) = p^2(t)$ shows that $q^2(t) \mid p^2(t)$, so replace $r(t) := \frac{p(t)}{q(t)} \in \mathbb{C}[t]$. Then we have the equation $a + bt^2 = r^2(t)$. We would then have

$$a + bt^2 = \left(\sum_{i=0}^{n} c_i t^i \right)^2$$

For some coefficients c_i with $c_n \neq 0$. The largest power of t appearing in the right hand series is just $c_n^2 t^{2n}$, and thus $n = 1$ (Since we may pass to an equality in $\mathbb{C}[t] \subset \mathbb{C}(t)$). This would claim that

$$a + bt^2 = (z + wt)^2 = z^2 + w^2 t^2 + zwt$$

From here we must have $zw = 0$, i.e. $z = 0$ or $w = 0$. For nonzero a, b, a quick check shows that neither of these cases work. In particular, $4 - 27t^2$ is not a square, thus $\mathrm{Gal}\big(\mathbb{C}(t)_f / \mathbb{C}(t)\big) = S_3$. I believe we can generalize the previous procedure to showing the Galois group of the splitting field of $X^3 - aX - bt$ over $\mathbb{C}(t)$ is S_3 for any nonzero a, b.