Bonus problem solutions 3

Additional info on the exam

In addition to the bonus problems, at least one of the exam problems will be closely related to the proofs of one of the following statements/theorems which we have covered.

- Lagrange's theorem.
- First isomorphism theorem for groups.
- A finite integral domain is a field (see Problem 6 on Pset 7).
- An element $\alpha \in \mathbb{C}$ is algebraic over $\mathbb{Q}$ if and only if $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is finite.
- There is a bijection between intermediate fields of a Galois extension and subgroups of the Galois group.

  (This is the Main Theorem, but not the normal subgroups part. Also you may assume the fixed field theorem, the characterizations of Galois extensions, etc.)
- The Galois group of the splitting field of an irreducible cubic f is A_3 if and only if the discriminant of f is a square.

Bonus problems

At least one of the exam problems will be closely related to one of the following.

Problem. Let K be the splitting field of $x^5 - 2$ over $\mathbb{Q}$. Show that the Galois group of $K/\mathbb{Q}$ is not isomorphic to S_5.

Solution. Let $\zeta = e^{2\pi i/5}$, and let $\alpha = \sqrt[5]{2}$ be the real fifth root of 2. The roots of $x^5 - 2$ are

$$\alpha_1 = \alpha,\ \alpha_2 = \alpha\zeta,\ \alpha_3 = \alpha\zeta^2,\ \alpha_4 = \alpha\zeta^3,\ \alpha_5 = \alpha\zeta^4.$$

Every element of $\mathrm{Gal}(K/\mathbb{Q})$ permutes the set $\{\alpha_1, \ldots, \alpha_5\}$, and is determined by its action on the roots. This lets us view $\mathrm{Gal}(K/\mathbb{Q})$ as a subgroup of S_5.

However, there is no element $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ which acts as the transposition (1 2), i.e., there is no automorphism σ such that

$$\sigma(\alpha_1) = \alpha_2, \quad \sigma(\alpha_2) = \sigma(\alpha_1), \quad \sigma(\alpha_i) = \alpha_i \quad \text{for} \quad 3 \le i \le 5.$$

This is because if σ were an automorphism, then we must have

$$\sigma(\alpha_1)\sigma(\alpha_3) = \sigma(\alpha_1\alpha_3) = \sigma(\alpha_2^2) = \sigma(\alpha_2)^2.$$

However, plugging in the values for each $\sigma(\alpha_i)$ given above, we see that

$$\alpha_2\alpha_3 = \alpha^2\zeta^3 \neq \alpha_1^2 = \alpha^2.$$

Thus, we have exhibited an element of S_5 which is not contained in $\mathrm{Gal}(K/\mathbb{Q})$, so $\mathrm{Gal}(K/\mathbb{Q})$ is not isomorphic to S_5.

Problem. Prove that the polynomial $x^4 - 10x^2 + 1$ is reducible in $\mathbb{F}_p[x]$ for every prime p.

Solution. The roots of $f = x^4 - 10x^2 + 1$ are $\pm\sqrt{5 \pm \sqrt{24}}$. If we compute the Galois group of the splitting field of this quartic, we find that it is D_2.

The idea is that there is no Galois extension of finite fields with automorphism group D_2. Degree 4 extensions of finite fields always have automorphism group C_4. Here is how we can prove the statement in the problem rigorously.

We note that $\sqrt{5 + \sqrt{24}} = \sqrt{2} + \sqrt{3}$. The key fact is that at least one of $\sqrt{2}$, $\sqrt{3}$, and $\sqrt{6}$ is already in $\mathbb{F}_p$.

1. If there exists $a \in \mathbb{F}_p$ with $a^2 = 2$, then

$$\begin{aligned} f &= (x - (a + \sqrt{3}))(x - (a - \sqrt{3}))(x - (-a + \sqrt{3}))(x - (-a - \sqrt{3})) \\ &= (x^2 - 2ax + (a^2 - 3))(x^2 + 2ax + (a^2 - 3)) \\ &= (x^2 - 2ax - 1)(x^2 + 2ax - 1), \end{aligned}$$

   so f is not irreducible.

2. The same argument works if there exists $b \in \mathbb{F}_p$ with $b^2 = 3$.

3. If there exists $c \in \mathbb{F}_p$ with $c^2 = 6$, then

$$\begin{aligned} f &= (x - \sqrt{5 + 2c})(x + \sqrt{5 + 2c})(x - \sqrt{5 - 2c})(x + \sqrt{5 - 2c}) \\ &= (x^2 - (5 + 2c))(x^2 - (5 - 2c)), \end{aligned}$$

   so f is not irreducible.

It remains to show that at least one of the above cases is true. Assume that both 2 and 3 are not squares in $\mathbb{F}_p$, so the polynomials $x^2 - 2$ and $x^2 - 3$ are both irreducible in $\mathbb{F}_p[x]$. So $\mathbb{F}_p[x]/(x^2 - 2)$ is isomorphic to $\mathbb{F}_p[x]/(x^2 - 3)$, since both are isomorphic to $\mathbb{F}_{p^2}$.

This means that the field $\mathbb{F}_p(\alpha)$ with $\alpha^2 = 2$ contains an element β with $\beta^2 = 3$. Then we must have $\beta = r\alpha$ for some $r \in \mathbb{F}_p$, so $\alpha\beta = 2r \in \mathbb{F}_p$. Since $(\alpha\beta)^2 = 6$, this shows that if 2 and 3 are not squares in $\mathbb{F}_p$, then 6 is a square in $\mathbb{F}_p$.

Note 1: To see that $\beta = r\alpha$, note that we have $\beta = r\alpha + s$ for some $r, s \in \mathbb{F}_p$. Squaring both sides, we get

$$3 = (2r^2 + s^2) + 2rs\alpha,$$

so either $r = 0$ or $s = 0$. We cannot have $r = 0$ because $s^2 = 3$ is impossible by assumption.

Note 2: Expressing the nested square root as a sum of unnested square roots is possible if and only if the Galois group is D_2 (as opposed to C_4 or D_4).