MATH 370 (Sp. 2025): ULA Exam I Review Session (with Lực Ta and Adam Wesley)

Remember to sign in, using either the QR code or this link.

Problem 1. Let F be a subfield of $\mathbb{C}$, and let K/F be a degree 2 extension. Is K/F necessarily Galois?

Solution. Yes. Since $F \subset \mathbb{C}$, HW2 problem 4 (Stewart 5.5) implies that $K = F(\sqrt{\lambda})$ for some $\lambda \in F$ (and $\sqrt{\lambda} \notin F$ by hypothesis). Thus, K is the splitting field of $x^2 - \lambda \in F[x]$. $\square$

Problem 2. Let $F \subset M \subset K$ be fields.

(a) Suppose K/F is Galois. Is K/M necessarily Galois?

Solution. Yes, by the fundamental theorem of Galois theory. $\square$

(b) Suppose K/F is Galois. Is M/F necessarily Galois?

Solution. No. Take $F = \mathbb{Q}$ and $M = \mathbb{Q}(^3\sqrt{2})$, and let K be the splitting field of $x^3 - 2$ (so that $K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$, where $\zeta_3 = \exp(2\pi i/3)$ is a third root of unity). Since K is the splitting field of an irreducible (by Eisenstein with $p = 2$) polynomial over $\mathbb{C}$, we know K/F is Galois. But M/F isn't Galois because $[M : F] = 3 \neq 1 = |\operatorname{Gal}(M/F)|$. $\square$

(c) Suppose M/F and K/M are both Galois. Is K/F necessarily Galois?

Solution. No. Take $F = \mathbb{Q}$, $M = \mathbb{Q}(\sqrt{2})$, and $K = \mathbb{Q}(\sqrt[4]{2})$. $\square$

Problem 3. Classify the Galois groups of the following polynomials.

(a) $f(x) := x^3 - 3x + 1$ over $\mathbb{Q}$.

Solution. It's irreducible by reduction modulo 2 (it's cubic, so it's reducible if and only if it has a root, which it doesn't in $\mathbb{F}_2$). So, a theorem from class says that the Galois group is $A_3 \cong Z_3$ if the discriminant is a square in $\mathbb{Q}$ and S_3 otherwise. Indeed, the discriminant is 81, so the Galois group is Z_3. $\square$

(b) The minimal polynomial of $\sqrt{2+i}$ over $\mathbb{Q}$.

Solution. Call this thing α. The minimal polynomial is $f(x) := x^4 - 4x^2 + 5$, which is irreducible over $\mathbb{Q}$; $f(x+1) = x^4 + 4x^3 + 2x^2 - 4x + 2$ is irreducible by Eisenstein with $p = 2$. (Alternatively, you could reduce modulo 2, check that $\overline{f}$ has no roots in $\mathbb{F}_2$, and then conclude that it also doesn't factor into irreducible quadratics since the only such quadratic over $\mathbb{F}_2$ is $x^2 + x + 1$, which doesn't square to $\overline{f}$.)

Thus, $\mathbb{Q}(\alpha)$ has degree 4, but is it the splitting field? Well, using the quadratic formula on $f(\sqrt{x})$, we find that the roots of f are $\pm\alpha$ and $\pm\beta$, where $\beta = \sqrt{2-i}$. In particular, the roots are all distinct, so by a problem from HW4, the form of f tells us that the Galois group is contained in D_4.

On the other hand, $\alpha\beta = \sqrt{5} \notin \mathbb{Q}(\alpha)$, so $\beta \notin \mathbb{Q}(\alpha)$, so the splitting field—which is $\mathbb{Q}(\alpha, \beta)$—isn't $\mathbb{Q}(\alpha)$. It follows that the Galois group has order greater than 4, but it's contained in D_4, so it has to be D_4. (Indeed, we have $i \in \mathbb{Q}(\alpha)$, so the minimal polynomial of β over $\mathbb{Q}(\alpha)$ is $x^2 - 2 + i$.) $\square$

(c) The minimal polynomial of $\sqrt{2+\sqrt{2}}$ over $\mathbb{Q}$.

Solution. Call this thing α, and call the splitting field K. To find $[K:\mathbb{Q}] = |\operatorname{Gal}(K/\mathbb{Q})|$, one can compute that α is a root of $x^4 - 4x^2 + 2$, which is irreducible over $\mathbb{Q}$ by Eisenstein with $p = 2$. So, $\mathbb{Q}(\alpha)$ has degree order 4.

But does K also have order 4? Well, let's find out what the roots are by using the quadratic formula on $x^2 - 4x + 2$. We get that the roots are $\pm\alpha$ and $\pm\beta$, where $\beta = \sqrt{2-\sqrt{2}}$, so $K = \mathbb{Q}(\alpha, \beta)$. By squaring α, we observe that $\mathbb{Q}(\alpha)$ contains $\sqrt{2}$. Does it also contain β? One litmus test is to see what $\alpha\beta$ is. It's actually $\sqrt{2}$, which, sure enough, is in $\mathbb{Q}(\alpha)$. Therefore, $\mathbb{Q}(\alpha) \ni \sqrt{2}/\alpha = \beta$. Hence, $\mathbb{Q}(\alpha) = K$, so the Galois group has order 4.

So, is it $Z_2 \times Z_2$ or Z_4? Well, consider the automorphism that sends α to β. Show that this automorphism has order greater than 2. Then, by Lagrange's theorem, it has order 4, so it generates the Galois group. □

(d) $f(x) := x^4 - 2$ over F, where F is the splitting field of $x^2 - 2$ over $\mathbb{Q}$.

Solution. Write $F = \mathbb{Q}(\sqrt{2})$. The splitting field of f over $\mathbb{Q}$ is $K := \mathbb{Q}(\sqrt[4]{2}, i) = F(\sqrt[4]{2}, i)$, and $\operatorname{Gal}(K/\mathbb{Q}) \leq D_4$ by a problem from HW4 (look at the form of f). It follows from the Tower Law that

$$|\operatorname{Gal}(K/F)| = [K:F] = \frac{[K:\mathbb{Q}]}{[F:\mathbb{Q}]} = \frac{|\operatorname{Gal}(K/\mathbb{Q})|}{2} \leq \frac{|D_4|}{2} = 4,$$

so $\operatorname{Gal}(K/F)$ is either 1, Z_2, Z_4, or $Z_2 \times Z_2$.

We claim that $\operatorname{Gal}(K/F) \cong Z_2 \times Z_2$. By the bound from above, it will suffice to just find two distinct elements of order 2, since that will imply that $Z_2 \times Z_2 \leq \operatorname{Gal}(K/F)$. Indeed, consider the maps $[\sqrt[4]{2} \mapsto -\sqrt[4]{2}, i \mapsto i]$ and $[\sqrt[4]{2} \mapsto \sqrt[4]{2}, i \mapsto -i]$. These are two valid automorphisms of order 2 that fix F, so we're done. (Note that $\sqrt[4]{2}$ can't be sent to $\pm i\sqrt[4]{2}$ since then $\sqrt{2} = (\sqrt[4]{2})^2$ would get sent to $(\pm i\sqrt[4]{2})^2 = -\sqrt{2}$, meaning that F wouldn't be fixed.)

Or, we can deduce that it's $Z_2 \times Z_2$ (as opposed to Z_4) by the fundamental theorem of Galois theory, since K has two distinct subextensions of degree 2 over F (which, by the fundamental theorem, correspond to two distinct subgroups of order 2 in $\operatorname{Gal}(K/F)$). □

(e) The same polynomial as in the last part, but now over $\mathbb{Q}$.

Solution. It's D_4. The previous part and the Tower Law imply that $[K:\mathbb{Q}] = 8$. The only subgroup of order 8 in S_4, thanks to Sylow II. □

Problem 4. Let K be a subfield of $\mathbb{R}$, and let $f \in K[x]$ be an irreducible polynomial. Show that if the Galois group of f has odd order, then the discriminant of f is positive.

Solution. Let's prove the contrapositive. Note that the discriminant of f can't be 0, since then f would have a repeated root, making it inseparable and thus (by virtue of the fact that $K \subset \mathbb{C}$) reducible.

So, suppose that the discriminant of f is negative. Then, by the definition of the discriminant in terms of the roots, at least one of the roots α is nonreal; since $K \subset \mathbb{R}$, it follows that $\overline{\alpha}$ is also a (distinct) root of f. Therefore, complex conjugation is an order 2 element of f (rather than an order 1 element), so by Lagrange's theorem, the Galois group has even order.

(Note that complex conjugation is always in the Galois group of a polynomial over a real ground field—sometimes as an order 1 element/the identity map, other times as an order 2 element—because complex conjugation fixes $\mathbb{R}$ and is a field automorphism of $\mathbb{C}$.) □

Problem 5. Let K/F be a Galois extension such that $\mathrm{Gal}(K/F) \cong Z_3 \times Z_{18}$. How many intermediate fields M are there such that

(a) $[M : F] = 18$

Solution. Four Z_3's, one generated by $(1,0)$ and the others generated by $(n,6)$ for $n = 0,1,2$. □

(b) $[M : F] = 27$

Solution. There's a unique Z_2, generated by $(0,9)$. To see that this is the unique one, note that in $Z_3 \times Z_{18} \cong Z_3 \times Z_9 \times Z_2$, there can't be any nonidentity elements of order dividing 2 inside the Z_3 or the Z_9. □

(c) $[M : F] = 3$

Solution. Four. There's one $Z_3 \times Z_6 \cong Z_3 \times Z_3 \times Z_2$, which we can see by writing $Z_3 \times Z_{18} \cong Z_3 \times Z_9 \times Z_2$. There are also three Z_{18}'s, namely those generated by $(n,1)$ for $n = 0,1,2$. □

(d) $[M : F] = 6$

Solution. Four. There's one $Z_3 \times Z_3$, namely $\langle (1,0),(0,6) \rangle$, and three Z_9's, namely those generated by $(n,2)$ for $n = 0,1,2$. □

(e) $\mathrm{Gal}(K/M) \cong Z_2$

Solution. This is the same as part (b). □

(f) $|\mathrm{Gal}(K/M)| = 6$

Solution. Four. Note that such a subgroup is an abelian group, so it must be isomorphic to $Z_6 \cong Z_3 \times Z_2$. So, you can reason through this one by decomposing $Z_3 \times Z_{18} \cong Z_3 \times Z_9 \times Z_2$ and using the previous parts. Or, you could note first that $(1,0)$ and $(0,9)$ generate a $Z_3 \times Z_2 \cong Z_6$. We also have three other copies of Z_6, each generated by $(n,3)$ for $n = 0,1,2$. □

(g) $\mathrm{Gal}(K/M) \cong Z_{27}$

Solution. None. □

(h) $|\mathrm{Gal}(K/M)| = 27$

Solution. Just one, generated by $(1,0)$ and $(0,2)$. □

Problem 6. True or false? Justify your answer.

(a) If $\alpha \neq \beta$ are both irrational, then $\mathbb{Q}(\alpha,\beta)$ is not a simple extension of $\mathbb{Q}$.

Solution. False. Take $\alpha = \sqrt{2}, \beta = 1 + \sqrt{2}$. [Exercise: these are distinct irrational numbers]. But then $\mathbb{Q}(\alpha,\beta) = \mathbb{Q}(\alpha)$ is a simple extension of $\mathbb{Q}$. □

(b) Every algebraic extension is finite.

Solution. False. Let $S = \{\sqrt{p_i} \mid p_i \in \mathbb{Z} \text{ is prime}\}$. Then $\mathbb{Q}(S)/\mathbb{Q}$ is algebraic, but does not have finite degree $\square$

(c) Two extensions of the same degree are isomorphic.

Solution. False. $\mathbb{Q}(\sqrt{2})/\mathbb{Q} \not\simeq \mathbb{Q}(\sqrt{3})/\mathbb{Q}$ because no element of the second field squares to 2. More formally, if $\varphi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3})$ is an isomorphism of extensions of $\mathbb{Q}$, then $2 = \varphi(2) = \varphi(\sqrt{2})^2$, but nothing in $\mathbb{Q}(\sqrt{3})$ squares to 2. $\square$

(d) Suppose there exist α and β such that the extensions $\mathbb{Q}(\alpha)/\mathbb{Q}$ and $\mathbb{Q}(\beta)/\mathbb{Q}$ are isomorphic. Then α and β have the same minimal polynomial over $\mathbb{Q}$.

Solution. False. Take $\alpha = \sqrt{2}, \beta = 1 + \sqrt{2}$. $\square$

Problem 7. Let $K/\mathbb{Q}$ be a Galois extension of degree 4 and suppose that $i \in K$. Prove that $\mathrm{Gal}(K/\mathbb{Q}) \simeq Z_2 \times Z_2$. *Hint: what can you say about the extension $K/\mathbb{Q}(i)$?*

Solution. First, since $K/\mathbb{Q}$ is Galois and $[K : \mathbb{Q}] = 4$, $|\mathrm{Gal}(K/\mathbb{Q})| = 4$, so $G := \mathrm{Gal}(K/\mathbb{Q}) \simeq Z_4$ or $G \simeq Z_2 \times Z_2$. Therefore we're done if we can show that there are distinct order two subgroups of G.

Second, observe by the tower law that $[K : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}] = 4$ so $[K : \mathbb{Q}(i)] = 2$. In particular, the correspondence tells us that G contains a normal subgroup of order 2.

Now, since K can be viewed as a subfield of $\mathbb{C}$, consider $\varphi : K \to \mathbb{C}$ defined by $\alpha \mapsto \bar{\alpha}$, where $\bar{\alpha}$ is the complex conjugate of α. We claim $\varphi \in \mathrm{Gal}(K/\mathbb{Q})$. First, since $\mathbb{Q}$ is real, φ fixes $\mathbb{Q}$. Also, φ is injective since K is a field. $\square$

Problem 8. Show that there are infinitely many irreducible polynomials over any field. *Hint: think about Euclid's proof that there are infinitely many primes in $\mathbb{Z}$.*

Solution. Let F be a field, and let $F[x]$ be its polynomial ring (in one variable). Suppose $L := \{f_1, f_2, \ldots, f_n\}$ is a collection of irreducible polynomials, then define $f = 1 + \prod_{i=1}^{n} f_i$. We may assume each f_i is monic, so f is. If f is irreducible, then $f \notin L$, because $\deg f > \max_i\{\deg f_i\}$. If f is not irreducible, then some monic irreducible polynomial $g|f$. But $g \neq f_i$ for any f_i; otherwise $f_i|1$ implying f_i is a constant, which is not irreducible. Therefore any finite list of irreducible polynomials misses at least one irreducible polynomial, so there must be infinitely many.

Note: if you start with the additional (very strong!) assumption that $|F| = \infty$, this proof can be done in one line; as a hint, consider what happens when $F = \mathbb{C}$.

Note 2: In the session on Tuesday, I (Adam) pointed out that you had to be careful in prime characteristic: while this is good advice in general, I myself was not sufficiently careful. That is, generalizing Euclid's argument works the exact same way–I just forgot that the product of irreducibles plus one doesn't have to be irreducible. Apologies for any confusion I may have caused. $\square$

You're doing great! :)