FINAL EXAM SOLUTIONS

Instructions: Justify your answers. You may use results from the homework sets and from class, but make sure to carefully state such results. No calculators and no notes allowed.

Grading: This exam is worth 30 points. You need a score of 12.5/30 or higher to pass this exam. More precisely, the following scale will be used:

A: $[26.5, 30]$, B: $[23, 26.5)$, C: $[19.5, 23)$, D: $[16, 19.5)$, E: $[12.5, 16)$, F: $[0, 12.5)$.

Problem 1. *Let $f(x) = x^5 - 3 \in \mathbf{Q}[x]$.*

(a) (1 point) Show that f is irreducible over $\mathbf{Q}$.
(b) (2 points) Give an explicit description of a splitting field L for f.
(c) (1 point) Compute $[L : \mathbf{Q}]$.
(d) (1 point) Show that $L/\mathbf{Q}$ is Galois.

Solution. (a) The polynomial $f(x)$ is irreducible over $\mathbf{Q}$ because it satisfies Eisenstein's criterion at $p = 3$.

(b) Let L be a splitting field of F. Since f is irreducible and $\mathbf{Q}$ has characteristic zero, f is separable. Let α, β be two distinct roots of f in L. Put $\zeta = \alpha/\beta$. Then ζ is a primitive 5th root of unity.

We claim $L = \mathbf{Q}(\alpha, \zeta)$. The above gives one inclusion: $\mathbf{Q}(\alpha, \zeta) \subset L$. On the other hand, $\zeta^j \alpha$, $0 \leq j \leq 4$ gives five distinct roots of f in $\mathbf{Q}(\alpha, \zeta)$. So f splits completely over $\mathbf{Q}(\alpha, \zeta)$. This gives the reverse inclusion $L \subset \mathbf{Q}(\alpha, \zeta)$.

(c) In general, the degree of a composite is at most the product of the degrees of its constituents. Thus $[\mathbf{Q}(\alpha, \zeta) : \mathbf{Q}] \leq [\mathbf{Q}(\alpha) : \mathbf{Q}][\mathbf{Q}(\zeta) : \mathbf{Q}] = 5 \cdot 4 = 20$. Since $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 5$ and $[\mathbf{Q}(\zeta) : \mathbf{Q}] = 4$ are relatively prime and both divide $[L : \mathbf{Q}]$, we have equality. Thus $[L : \mathbf{Q}] = 20$

(d) The splitting field of a separable polynomial is Galois. We have seen that f is irreducible and separable. Thus its splitting field L is Galois over $\mathbf{Q}$. □

E-mail address: `wgoldring@math.su.se`.

Problem 2. *Let* $f(x) = x^5 - 3 \in \mathbf{Q}[x]$ *and* L *be as in* Problem 1.

(a) *(3 points) Give generators and relations for* $\mathrm{Gal}(L/\mathbf{Q})$.
(b) *(2 points) Show that* $\mathrm{Gal}(L/\mathbf{Q})$ *is solvable.*
(c) *(1 point) Show that* f *is solvable by radicals.*
(d) *(1 point) Let* α *be a root of* f *in* L. *Is* α *constructible by straightedge and compass? Explain.*

Solution. Let $G = \mathrm{Gal}(L/\mathbf{Q})$.

(a) Since α and ζ generate $L/\mathbf{Q}$, an automorphism of $L/\mathbf{Q}$ is determined by its action on α and ζ. Since an automorphism must map a root of an irreducible polynomial in $\mathbf{Q}[x]$ to another root of the same polynomial, every automorphism of L must have the form

$$\begin{cases} \zeta & \mapsto & \zeta^k, & 1 \le k \le 4 \\ \alpha & \mapsto & \zeta^j\alpha, & 0 \le j \le 4 \end{cases} \tag{1}$$

This collection gives at most 20 automorphisms. Since $L/\mathbf{Q}$ is Galois, the order of G equals the degree of $L/\mathbf{Q}$, which was seen to be 20. Thus every map in (1) must define an automorphism of L.

Define $\sigma, \tau \in G$ by

$$\begin{cases} \sigma(\zeta) = \zeta^2 \\ \sigma(\alpha) = \alpha \end{cases} \text{and} \begin{cases} \tau(\zeta) = \zeta \\ \tau(\alpha) = \alpha\zeta \end{cases}. \tag{2}$$

and $\tau(\zeta) = \zeta$, $\tau(\alpha)$ Then σ has order 4 and τ has order 5 in G. Let $N = \langle \tau \rangle$. Then N is a subgroup of G of order 5.

We claim that N is normal in G. This will be confirmed by direct computation below, but it also follows from Sylow's Theorem: In fact, N is a 5-Sylow subgroup of G and the number of 5-Sylow subgroups in G is $\equiv 1 \pmod 5$ and divides 4, hence equals 1.

Since N is normal in G, it remains only to compute the action of σ on N by conjugation. To do this, it suffices to compute $\sigma\tau\sigma^{-1}$ on the generators ζ, α of L. One finds $\sigma\tau\sigma^{-1}(\zeta) = \zeta$ and $\sigma\tau\sigma^{-1}(\alpha) = \sigma\tau(\alpha) = \sigma(\alpha\zeta) = \alpha\zeta^2$. Thus $\sigma\tau\sigma^{-1} = \tau^2$. In sum, generators and relations for G are given by

$$G = \langle \sigma, \tau | \sigma^4 = \tau^5 = 1, \sigma\tau\sigma^{-1} = \tau^2 \rangle.$$

(b) Since N is cyclic, it is solvable. Since G/N has order 4, it is abelian, hence cyclic. If H is any group and K is a normal subgroup of H, then H is solvable if and only if both K and H/K are solvable. Applying this with $H = G$ and $K = N$ gives that G is solvable.

More or less equivalently, the filtration $\{1\} \subset N \subset G$ satisfies the definition of solvability: each group is normal in the next one and the quotients are all abelian.

(c) Solution 1: A separable polynomial is solvable by radicals if and only if its Galois group is solvable. So f is solvable by radicals by (b).

Solution 2: if K/F is a finite separable extension and $\alpha \in K$, then α is solvable by radicals starting from F if there is a filtration of K by subfields F_i such that each successive extension F_{i+1}/F_i is obtained by adding to F_i a root of $x^n - a$ for some $a \in F_i$. The roots of $x^5 - 3$ are all obtained in this way in one step, where $n = 5$ and $a = 3$. So we also see directly that f is solvable by radicals.

Using the reverse direction of "A separable polynomial is solvable by radicals if and only if its Galois group is solvable" we obtain a new solution to (b).

(d) If an algebraic number is constructible by straightedge and compass, its degree must be a power of 2. Since the degree of the roots of f is 5, the roots of f are not constructible by straightedge and compass.

□

Problem 3. *Let ζ_7 be a primitive 7th root of unity in a field of characteristic zero.*

(a) (1 point) Show that $\mathbf{Q}(\zeta_7)/\mathbf{Q}$ is Galois.
(b) (2 points) Give an explicit description of $\mathrm{Gal}(\mathbf{Q}(\zeta_7)/\mathbf{Q})$
(c) (2 points) Let $\alpha = \zeta_7 + \zeta_7^2 + \zeta_7^4$. Find $m_{\alpha,\mathbf{Q}}(x)$.
(d) (2 points) Let $\gamma = \zeta_7 + \zeta_7^{-1}$. Find $m_{\gamma,\mathbf{Q}}(x)$.
(e) (1 point) Find $m_{\zeta_7,\mathbf{Q}(\gamma)}(x)$.

Proof. (a) By definition of "primitive" every 7th root of unity is a power of ζ_7. Therefore $\mathbf{Q}(\zeta_7)$ is a splitting field of the separable polynomial $x^7 - 1$ over $\mathbf{Q}$; hence $\mathbf{Q}(\zeta_7)/\mathbf{Q}$ is Galois.

(b) One has a canonical isomorphism between $(\mathbf{Z}/7)^\times$ and $\mathrm{Gal}(\mathbf{Q}(\zeta_7)/\mathbf{Q})$: Given $a \in (\mathbf{Z}/7)^\times$ define $\sigma_a : \mathbf{Q}(\zeta_7) \to \mathbf{Q}(\zeta_7)$ by $\sigma_a(\zeta_7) = \zeta_7^a$. Since the 7th cyclotomic polynomial $\Phi_7(x)$ is irreducible and ζ_7, ζ_7^a are both roots of it, there exists an isomorphism $\mathbf{Q}(\zeta_7) \simeq \mathbf{Q}(\zeta_7^a)$ mapping ζ_7 to ζ_7^a. But $\mathbf{Q}(\zeta_7^a) = \mathbf{Q}(\zeta_7)$ so this isomorphism is σ_a. Thus σ_a is an automorphism. On the other hand, every automorphism is determined by its action on the primitive element ζ_7, so we see that $a \mapsto \sigma_a$ defines an isomorphism as claimed.

(c) The element α is the sum of the ζ_7^a as a ranges over the squares in $\mathbf{F}_7^\times$. Therefore $\mathbf{Q}(\alpha)$ is the fixed field of the index 2 subgroup $(\mathbf{F}_7^\times)^2 = \{1, 2, 4\}$ of $\mathbf{F}_7^\times$. Thus the degree of α over $\mathbf{Q}$ is 2 and the other root of its minimal polynomial is $\beta := \zeta_7 + \zeta_7^3 + \zeta_7^6$; this is the sum of the non-square powers of ζ_7. Thus

$$m_{\alpha,\mathbf{Q}}(x) = (x - \alpha)(x - \beta) = x^2 - (\alpha + \beta)x + \alpha\beta$$

The sum $\alpha + \beta$ is $\zeta_7 + \cdots + \zeta_7^6 = -1$ since $\Phi_7(x) = x^6 + \cdots + x + 1$. As for the product, we find

$$\alpha\beta = 3 + \zeta_7 + \cdots + \zeta_7^6 = 3 - 1 = 2,$$

i.e., 3 terms are equal to 1 and every term different from 1 appears once when we expand as a sum of powers of ζ_7. Therefore $m_{\alpha,\mathbf{Q}}(x) = x^2 + x - 2$.

(d) Similar to (c), one has that $\mathbf{Q}(\gamma)$ is the fixed field of the index 3 subgroup $\{1, -1\}$ of $\mathbf{F}_7^\times$ (it is the subgroup of cubes). So the other roots of $m_{\gamma,\mathbf{Q}}(x)$ will be $\delta = \zeta_7^2 + \zeta_7^{-2}$ and $\epsilon = \zeta_7^3 + \zeta_7^{-3}$. One computes the values of the three elementary symmetric functions in γ, δ, ϵ: As before, the sum $\gamma + \delta + \epsilon = -1$. When we expand $\gamma\delta + \gamma\epsilon + \delta\epsilon$, no term is equal to 1. Since we have $4 \cdot 3 = 12$ terms total, the expression must be $2(\zeta_7 + \cdots + \zeta_7^6) = -2$, since we know the value is rational and that $\zeta_7, \ldots \zeta_7^6$ is a basis for $\mathbf{Q}(\zeta_7)/\mathbf{Q}$.

Finally, the product $\gamma\delta\epsilon = 2 + \zeta_7 + \ldots + \zeta_7^6 = 2 - 1 = 1$ (and we don't even have to multiply out the terms since we know the number of non-1 terms must be divisible by 6; since it is not 0 it must be 6).

Thus $m_{\gamma,\mathbf{Q}}(x) = x^3 + x^2 - 2x - 1$.

(e) The polynomial

$$(x - \zeta_7)(x - \zeta_7^6) = x^2 - (\zeta_7 + \zeta_7^6)x + 1$$

has coefficients in $\mathbf{Q}(\gamma)$. To conclude it is the minimal polynomial, it suffices to show that ζ_7 does not belong to $\mathbf{Q}(\gamma)$. By checking which σ_a fix γ, we find that $\mathrm{Gal}(\mathbf{Q}(\zeta_7)/\mathbf{Q}(\gamma) = \{\sigma_1, \sigma_{-1}\}$. So $[\mathbf{Q}(\zeta_7) : \mathbf{Q}(\gamma)] = 2$. $\square$

Problem 4.

(a) *(2 points) Construct a Galois extension of* $\mathbf{Q}$ *with Galois group* $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

(b) *(1 point) Let* $g(x) = x^3 - 2x + 4 \in \mathbf{Q}[x]$. *What subgroup of* S_3 *is isomorphic to* $\mathrm{Gal}(g)$*? Explain.*

(c) *(2 points) Now view* $g(x)$ *as a polynomial in* $\mathbf{Q}(i)[x]$*, where* i *is a square root of* -1*. What subgroup of* S_3 *is isomorphic to* $\mathrm{Gal}(g)$ *in this case?*

Proof. (a) We pick two primes $5, 13$ congruent to 1 modulo 4 and the prime 3 congruent to 1 modulo 2. We will construct our extension as a subfield of $\mathbf{Q}(\zeta_N)$ where $N = 3 \cdot 5 \cdot 13 = 195$ and ζ_N is a primitive Nth root of unity. We seek a subgroup H of $\mathrm{Gal}(\mathbf{Q}(\zeta_N)/\mathbf{Q})$ such that the fixed field $\mathbf{Q}(\zeta_N)^H$ will have desired properties. Since $\mathrm{Gal}(\mathbf{Q}(\zeta_N)/\mathbf{Q}) = (\mathbf{Z}/N)^\times$ is abelian, all of its subgroups are normal. By the fundamental correspondence of Galois theory, the fixed field $\mathbf{Q}(\zeta_N)^H$ is Galois over $\mathbf{Q}$ and its Galois group is $(\mathbf{Z}/N)^\times/H$. By the Chinese remainder theorem,

$$(\mathbf{Z}/N)^\times \cong (\mathbf{Z}/3)^\times \times (\mathbf{Z}/5)^\times \times (\mathbf{Z}/13)^\times \cong \mathbf{Z}/2 \times \mathbf{Z}/4 \times \mathbf{Z}/12.$$

So we want H to be a subgroup of order 3 of $(\mathbf{Z}/N)^\times$ such that the quotient is $\mathbf{Z}/4 \times \mathbf{Z}/4 \times \mathbf{Z}/2$. Let H_0 be the unique subgroup of $(\mathbf{Z}/13)^\times$ of order 3 (equivalently index 4; it is the subgroup of 4th powers). Let H be the subgroup of $(\mathbf{Z}/N)^\times$ where the $(\mathbf{Z}/3)^\times$ and $(\mathbf{Z}/5)^\times$ components are equal to 1 and where we require the component in $(\mathbf{Z}/13)^\times$ to belong in H_0. Then $H \cong H_0 \cong \mathbf{Z}/3$ and $(\mathbf{Z}/N)^\times/H \cong \mathbf{Z}/4 \times \mathbf{Z}/4 \times \mathbf{Z}/2$. Note that $(\mathbf{Z}/13)^\times/H_0$ has order 4 and is cyclic as every quotient of a cyclic group is cyclic.

(b) Dangerous curve ahead: Polynomials which may appear to be irreducible for some reason may be reducible unless proven otherwise!

Applying the Rational Root Test, we find that -2 is a root. Factoring gives $g(x) = (x+2)(x^2-2x+2)$. The quadratic factor is irreducible over $\mathbf{Q}$ because its discriminant is $2^2 - 4 \cdot 2 = -4$ is not a square in $\mathbf{Q}$. Therefore the Galois group of G is cyclic of order 2; it is the transposition of the two roots of the quadratic factor (which fixes the root -2 as it must).

(c) In $\mathbf{Q}(i)$, the discriminant is a square: $-4 = (2i)^2$. So the Galois group is trivial over $\mathbf{Q}(i)$. □

Problem 5. *Let* $h(x) = x^{12} + x^{11} + \cdots + x + 1 \in \mathbf{Z}[x]$.

(a) *(1 point) Suppose* p *is a prime,* $p \equiv 1 \pmod{13}$. *Show that* $h(x)$ *splits completely in* $\mathbf{F}_p[x]$.

(b) *(2 points) Suppose* p *is a prime,* $p \equiv 2 \pmod{13}$. *Show that* $h(x)$ *is irreducible in* $\mathbf{F}_p[x]$.

(c) *(2 points) Show that* $x^3 - x + 2$ *divides* $x^{125} - x$ *in* $\mathbf{F}_5[x]$. Note: *Long division is highly discouraged in this problem.*

Proof. One has $h(x) = \Phi_{13}(x)$ and parts (a), (b) are special cases of the factorization of the cyclotomic polynomial $\Phi_N(x)$ modulo a prime which doesn't divide N.

(a) If $p \equiv 1 \pmod{13}$, then $x^{13} - 1$ divides $x^{p-1} - 1$, so $h(x)$ divides $x^{p-1} - 1$. Since the latter splits completely over $\mathbf{F}_p$ (having all nonzero elements of $\mathbf{F}_p$ as roots, each with multiplicity one), so does its factor $h(x)$.

(b) Since $2^{(13-1)/2} = 2^6$ and $2^{(13-1)/3} = 2^4$ are not 1 mod 13, one has that 2 generates $\mathbf{F}_{13}^\times$. Assume $h(x)$ has an irreducible factor $q(x)$ of degree d. Then a root α of $q(x)$ generates $\mathbf{F}_{p^d}$. But every root of $x^{13} - 1$ is a 13th root of unity, hence a power of the primitive root α. Therefore $x^{13} - 1$ splits in $\mathbf{F}_{p^d}$. So every root of $x^{13} - 1$ is also a root of $x^{p^d} - x$. Since $x^{13} - 1$ is separable over $\mathbf{F}_p$, we conclude that $x^{13} - 1$ divides $x^{p^d - 1} - 1$. Hence 13 divides $p^d - 1$. So $2^d \equiv p^d \equiv 1 \pmod{13}$ since $p \equiv 2 \pmod{13}$. Since 2 is a generator mod 13, one has $d = 12$ (as $12|d$ and $d \leq 12$).

(c) The polynomial $x^3 - x + 2$ has no root in $\mathbf{F}_5$. Since its degree is ≤ 3, we conclude it is irreducible over $\mathbf{F}_5$. The polynomial $x^{5^3} - x = x^{125} - x$ factors over $\mathbf{F}_5$ as the product of all irreducible polynomials in $\mathbf{F}_5[x]$ of degree 1 or 3 (each with multiplicity one, though this extra detail is not required for the problem). Hence $x^3 - x + 2$ divides $x^{125} - x$.

$\square$