FINAL EXAM SOLUTIONS

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

Grading: This exam is worth 30 points. If you completed homework assignments, your homework bonus (out of 3 points) will be added to your score. 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 $f(x) = x^7 - 20 \in \mathbf{Q}[x]$.*

(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 over $\mathbf{Q}$.
(c) (1 point) Compute $[L : \mathbf{Q}]$. Justify your answer.
(d) (1 point) Show that $L/\mathbf{Q}$ is Galois.

Solution. (a) The polynomial f is irreducible since it is Eisenstein at the prime $p = 5$.

(b) A splitting field L for f is given by adjoining to $\mathbf{Q}$ a root α of $x^7 - 20$ and a primitive 7th root of unity ζ. Since the derivative of f is $7x^6$, the polynomial f shares no nontrivial common factor with its derivative; hence f is separable. The 7 distinct roots of f are $\alpha\zeta^j$ with $0 \leq j \leq 6$. So they are all in L. Conversely, any splitting field must contain all the roots of f, in particular must contain α and another root β of f. Then α/β is a 7th root of 1 and not equal to 1; hence α/β is a primitive 7th root of 1. Every other 7th root of 1 is a power of α/β. In particular, any splitting field contained in L must contain both α and ζ.

(c) One has $[L : \mathbf{Q}] = 7 \cdot 6 = 42$, since $L = \mathbf{Q}(\alpha, \zeta)$, $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 7$, $[\mathbf{Q}(\zeta), \mathbf{Q}] = 6$ and 7 and 6 are relatively prime.

(d) A splitting field of a separable polynomial is Galois. We have seen in (b) that L is a splitting field of f and that f is separable. Hence $L/\mathbf{Q}$ is a Galois. □

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

Problem 2. *Let f and L be as in Problem 1.*

(a) (2 points) Give generators and relations for $\mathsf{Gal}(L/\mathbf{Q})$*.*
(b) (2 points) Show that $\mathsf{Gal}(L/\mathbf{Q})$ *is solvable.*
(c) (2 points) Show that there is a unique extension $K/\mathbf{Q}$ of degree 6 which is contained in L.
(d) (2 poins) Show that there is a unique quadratic extension $F/\mathbf{Q}$ contained in L and describe F as $\mathbf{Q}(\sqrt{D})$ for some integer D.

Solution. (a) Every automorphism of $L/\mathbf{Q}$ must map a root of an irreducible polynomial with $\mathbf{Q}$-coefficients to a root of that same polynomial. In particular, every automorphism must map α to $\alpha\zeta^j$ with $0 \leq j \leq 6$ and map ζ to ζ^k, with $1 \leq k \leq 6$. Since $L/\mathbf{Q}$ is Galois of degree 42, it has that many automorphisms. Hence all of the 42 choices above give well-defined automorphisms. Define $\sigma \in \mathsf{Gal}(L/\mathbf{Q})$ by $\sigma(\alpha) = \alpha$ and $\sigma(\zeta) = \zeta^3$ (we choose ζ^3 because 3 is a generator of $(\mathbf{Z}/7)^\times$). Define $\tau \in \mathsf{Gal}(L/\mathbf{Q})$ by $\tau(\alpha) = \zeta\alpha$ and $\tau(\zeta) = \zeta$. One computes the action of conjugation of σ on τ by computating the conjugation on the generators α, ζ: One finds

$$\sigma\tau\sigma^{-1} = \tau^3.$$

Hence a presentation by generators and relations is given by

$$\mathsf{Gal}(L/\mathbf{Q}) = \langle \sigma,\ \tau \mid \sigma^6 = \tau^7 = 1,\ \sigma\tau\sigma^{-1} = \tau^3 \rangle.$$

(b) Solution 1: The polynomial f determines a simple radical extension. Hence its splitting field is solvable, since $\mathbf{Q}$ has characteristic 0. Since $L/\mathbf{Q}$ is solvable by radicals, its Galois group is solvable.

Solution 2: Let $N = \langle \tau \rangle$. Then N is a normal subgroup of $\mathsf{Gal}(L/\mathbf{Q})$ (seen either directly from the presentation or via Sylow's theorem, as N is the necessarily unique 7-Sylow subgroup of $\mathsf{Gal}(L/\mathbf{Q})$. Now $\mathsf{Gal}(L/\mathbf{Q})/N \cong \langle \sigma \rangle$ is cyclic of order 6. Since N and $\mathsf{Gal}(L/\mathbf{Q})/N$ are both solvable, so is $\mathsf{Gal}(L/\mathbf{Q})$.

(c) By the Galois correspondence, an extension $K/\mathbf{Q}$ of degree 6 is the fixed field of a subgroup of $\mathsf{Gal}(L/\mathbf{Q})$ of order 7. Such a subgroup is a 7-Sylow. By Sylow's theorem, the number of 7-Sylows is 1 mod 7 and divides 6, hence is 1. So there is a unique subgroup of order 7 and a unique extension K/Q of degree 6, which is $K = \mathbf{Q}(\zeta)$.

(d) By the correspondence, a quadratic extension $F/\mathbf{Q}$ is the fixed field of a subgroup H of order 21. Such a subgroup H again contains a unique 7-Sylow, so $N \subset H$. Since the correspondence is inclusion-reversing, $F \subset K$. But $K = \mathbf{Q}(\zeta)$. We have seen in class that if p is an odd prime and ζ_p is a primitive pth root of 1, then the unique quadratic extension of $\mathbf{Q}$ contained in $\mathbf{Q}(\zeta_p)$ is $\mathbf{Q}(\sqrt{p})$ if $p \equiv 1 \pmod 4$ and $\mathbf{Q}(\sqrt{-p})$ if $p \equiv 3 \pmod 4$. Hence $F = \mathbf{Q}(\sqrt{-7})$.

□

Problem 3. *Let $\Phi_{15}(x) \in \mathbf{Z}[x]$ be the cyclotomic polynomial of primitive 15th roots of unity. Let ζ be a root of $\Phi_{15}(x)$ in some finite extension of $\mathbf{Q}$.*

(a) (2 points) Show that for every prime p, the reduction of $\Phi_{15}(x)$ modulo p is reducible in $\mathbf{F}_p[x]$.
(b) (1 point) Is the regular 15-gon constructible by straightedge and compass? Justify your answer.
(c) (2 point) Show that there are precisely three quadratic extensions of $\mathbf{Q}$ contained in $\mathbf{Q}(\zeta)$.
(d) (2 points) Describe the three distinct quadratic extensions of $\mathbf{Q}$ contained in $\mathbf{Q}(\zeta)$ in the form $\mathbf{Q}(\sqrt{D})$, where $D \in \mathbf{Z}$ is an integer.

Solution. (a) The reducibility is easier for $p = 3, 5$: One has $x^{15} - 1 = (x^3 - 1)^5$ and $x^{15} - 1 = (x^5 - 1)^3$ in characteristic 5, 3, respectively. On the other hand, the degree of Φ_{15} is $\varphi(15) = 8$ and we see that $x^{15} - 1$ does not have an irreducible degree 8 factor modulo 3 or 5.

From now on, assume $p \neq 3, 5$, so that $(p, 15) = 1$. One has

$$\mathsf{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q}) = (\mathbf{Z}/15)^\times = (\mathbf{Z}/3)^\times \times (\mathbf{Z}/5)^\times \cong \mathbf{Z}/2 \times \mathbf{Z}/4$$

(all but the last isomorphism are canonical, so we may write "="). Hence the exponent of $\mathsf{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$ is 4 i.e., the 4th power of every element is the identity. Thus $p^4 \equiv 1 \pmod{15}$ for every prime $p \neq 3, 5$. This gives the chain of divisibility relations

$$x^{15} - 1 \mid x^{p^4 - 1} - 1 \mid x^{p^4} - x.$$

The rightmost polynomial factors as the product of all irreducible polynomials over $\mathbf{F}_p$ of degree dividing 4 (each appearing once). Hence all factors of $x^{15} - 1 \bmod p$ have degree dividing 4.

(b) Yes, the regular 15-gon is constructible by straightedge and compass, because 15 is the product of two distinct Fermat primes $3 = 2^{2^0} + 1$ and $5 = 2^{2^1} + 1$.

(c) By the above description of the Galois group, it has precisely three quotients of order 2; these correspond to the three quadratic extensions of $\mathbf{Q}$ contained in $\mathbf{Q}(\zeta)$ by the Galois correspondence.

(d) Using what we learned about cyclotomic extensions, esp. $\mathbf{Q}(\zeta_p)$ where p is an odd prime and ζ_p is a primitive pth root of 1, we know that $\mathbf{Q}(\sqrt{5}) \subset \mathbf{Q}(\zeta_5)$ and $\mathbf{Q}(\sqrt{-3}) \subset \mathbf{Q}(\zeta_3)$ (in fact here we have a coincidental equality special to $p = 3$) since $5 \equiv 1 \pmod 4$ and $3 \equiv 3 \pmod 4$. Hence the third quadratic subfield is $\mathbf{Q}(\sqrt{-3} \cdot \sqrt{5}) = \mathbf{Q}(\sqrt{-15})$. □

Problem 4.

(a) *(2 points) Let p be a prime, let $a \in \mathbf{F}_p^\times$ and put $g(x) = x^p - x + a$. Show that $g(x)$ is irreducible in $\mathbf{F}_p[x]$.*

(b) *(2 points) Let G be a subgroup of S_5 which contains a 5-cycle and a transposition. Show that $G = S_5$.*

(c) *(2 points) Assume k is an integer which is divisible by 3 and not divisible by 5. Show that the Galois group of $h(x) = x^5 - x + k \in \mathbf{Q}[x]$ is S_5.*

Solution 1 of (a). Let α be a root of g in an extension of $\mathbf{F}_p$. An automorphism takes a root of an irreducible polynomial to another root of the same irreducible polynomial. Apply this to the Frobenius automorphism: One has $\mathsf{Frob}(\alpha) = \alpha^p = \alpha - a$. Iterating gives $\mathsf{Frob}^k(\alpha) = \alpha - ka$. Hence $\alpha - ka$ and α have the same minimal polynomial for all $k \geq 1$. Since $a \in \mathbf{F}_p^\times$, every $b \in \mathbf{F}_p$ is a positive integer multiple of a. Hence the minimal polynomial of α has the p distinct roots $\alpha, \alpha+1, \ldots, \alpha+p-1$. So the minimal polynomial is g by degree considerations. □

Solution 2 of (a). If α is a root of g in some extension, then one checks by plugging in that so are $\alpha, \alpha+1, \ldots \alpha+p-1$. So these are the p distinct roots of g which necessarily exhaust all the roots of g since $\deg g = p$. Hence $\mathbf{F}_p(\alpha) = \mathbf{F}_p(\beta)$ for any two roots α, β (since $\beta - \alpha \in \mathbf{F}_p$). Thus every root of g generates an extension of the same degree as every other root. So all the factors of g have the same degree, call it d. If the number of factors is e, then $p = de$. Since p is prime $d = 1$ or $e = 1$. But g has no roots in $\mathbf{F}_p$, since $b^p = b$ for all $b \in \mathbf{F}_p$. Hence $e = 1$ and g is irreducible of degree $d = p$. □

Solution of (b). The order G is divisible by 10 and divides 120. Further S_5 has no subgroup of index $k < 5$ except A_5, as such would give a non-trivial homomorphism $S_5 \to S_k$ which can only be $\mathrm{sgn} : S_5 \to \{\pm 1\}$ with kernel A_5. Thus, either $G = S_5$ as desired, or $|G|$ must be 10 or 20. In the latter two cases, G has a normal 5-Sylow subgroup. so G is a subgroup of the normalizer of a 5-Sylow of S_5. Since all 5-Sylows are conjugate, so are their normalizers. Writing one down, the normalizer of $\langle (12345) \rangle$ is

$$\langle (12345), (2354) \mid (12345)^5 = (2354)^4 = 1,\ (2354)(12345)(2354)^{-1} = 12345)^2 \rangle$$

In particular, we see that all elements of order 2 in the normalizer have type $(2,2)$, so the normalizer contains no transpositions. □

Solution of (c). Here we use the method of producing cycle types in the Galois group over $\mathbf{Q}$ by reducing our polynomial with $\mathbf{Z}$ coefficients modulo primes which don't divide the discriminant.

Using the formula for the discriminant of a trinomial $x^n + ax + b$, we find that the discriminant of h is $-4^4 + 5^5 k^4$; it is relatively prime to 3 and 5 since $3|k$.

By part (a), h is irreducible mod 5 (since $(5,k) = 1$). Hence the Galois group of h over $\mathbf{Q}$ contains a 5-cycle. Since $3|k$, the reduction of h mod 3 is

$$x^5 - x = x(x^4 - 1) = x(x+1)(x-1)(x^2+1)$$

and $x^2 + 1$ is irreducible mod 3 since it has degree < 4 and has no roots in $\mathbf{F}_3$. Hence the Galois group of h over $\mathbf{Q}$ contains a transposition. By part (b), the Galois group is S_5. □

Problem 5.

(a) (1 point) Show that $x^4 + x + 1$ *divides* $x^{16} - x$ *in* $\mathbf{F}_2[x]$.
(b) (1 point) Show that $x^4 + x + 1$ *divides* $x^{27} - x$ *in* $\mathbf{F}_3[x]$.
(c) (1 point) Show that the Galois group of $x^4 + 7x + 1 \in \mathbf{Q}[x]$ *is* S_4.
(d) (1 point) Let α *be a real root of* $x^4 + 7x + 1$. *Show that* α *is not constructible by straightedge and compass.*

Solution. In $\mathbf{F}_p[x]$, one has that $x^{p^n} - x$ is the product of all irreducible polynomials of degree dividing n, each appearing with multiplicity one.

(a) By the general fact above, it is enough to show that $x^4 + x + 1$ is irreducible over $\mathbf{F}_2$. It visibly has no roots. The only other option would be that it would factor as a product of two irreducible quadratic polynomials. The only irreducible quadratic polynomial over $\mathbf{F}_2$ is x^2+x+1, so we conclude by observing that $(x^2 + x + 1)^2 \neq x^4 + x + 1$ (e.g., compare coefficients of x).

(b) Plugging in, we see that 1 is a root. Dividing out by $x - 1$, the remaining cubic has no roots, hence is irreducible. So $x^4 + x + 1$ is the product of a linear factor and an irreducible cubic.

(c) We use the method of 4(c). The discriminant is relatively prime to $2, 3$.

Notice that $x^4 + 7x + 1 \equiv x^4 + x + 1 \pmod 2$ and $\pmod 3$ and the factorizations of $x^4 + x + 1$ in $\mathbf{F}_2[x]$ and $\mathbf{F}_3[x]$ were determined in (a) and (b). Hence the Galois group over $\mathbf{Q}$ contains a 4-cycle and a 3-cycle. A subgroup of S_4 which contains a 4-cycle and a 3-cycle is all of S_4, for its order is divisible by 12 and it can't be A_4 due to the odd 4-cycle.

(d) We have to show that $\mathbf{Q}(\alpha)$ does not contain a quadratic extension of $\mathbf{Q}$. By the Galois correspondence and part (c), this is equivalent to showing that a subgroup of S_4 of order 6 is not contained in a subgroup of order 12. We conclude noting that the only subgroup of S_4 of order 12 is A_4 and that A_4 has no subgrou of order 6.

□