FINAL EXAM SOLUTIONS

Must be submitted, preferably by the course website, else by email, at the latest by:
16:00 on 2020-12-18 (unless you have been granted extra time)

1. Instructions

Justify your answers. Since this is an exceptional "zoom-pandemic-exam" you may use notes, homework and texts associated with the course (tablet notes on the course website, the text by Dummit & Foote), but you should not search on the internet for answers. You may e.g., use part of Problem 4 to do part of Problem 1, even if you are unsuccessful with that part of Problem 4. You may use part (a) of a problem to do part (b) even if you have not solved (a), and so on. You can say "By Homework 3, problem 2,...". You do not need to restate the question in your solution. **Please email me if you have any questions during the exam**.

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: $[0, 12.5)$.

2. Problems

There are 5 problems:

Problem 1 (5 points)**.** *Let $f(x) = x^{11} - 29 \in \mathbf{Q}[x]$.*

(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 over $\mathbf{Z}$ since it is Eisenstein at the prime $p = 29$. Hence f is irreducible over $\mathbf{Q}$ by Gauss' Lemma.

(b) Let ζ be a primitive 11th root of unity and let α be a root of f, both in some extension of $\mathbf{Q}$. Set $L := \mathbf{Q}(\alpha, \zeta)$. Then we claim L is a splitting field of f. The roots of f are the $\zeta^i \alpha$ with $i \in \mathbf{Z}/11$. So f splits completely over L.

The polynomial f is separable, because every irreducible polynomial over a field of characteristic zero is so; or, more directly, the derivative of f is $11x^{10}$, so we see that f is relatively prime to its derivative, hence separable, over any field of characteristic not $3, 5$ or 13. So let β be another root of f, distinct from α. Then α/β is not 1 but is a root of $x^{11} - 1$; whence α/β is a primitive 11th root of unity (since 11 is prime). Any subfield of L over which f splits must contain α, β, so it must also contain a primitive 11th root of unity, so it contains all 11th roots of unity, so it contains L.

(c) The degree of a composite is always at most the product of the degrees, so

$$[L : \mathbf{Q}] \leq [\mathbf{Q}(\zeta) : \mathbf{Q})][\mathbf{Q}(\alpha) : \mathbf{Q}] = 10 \cdot 11 = 110.$$

Since $10, 11$ are relatively prime, we have equality by the multiplicativity of degrees in towers. So $[L : \mathbf{Q}] = 10 \cdot 11 = 110$.

(d) A finite extension is Galois if and only if it is the splitting field of some separable polynomial. Since L is the splitting field of f over $\mathbf{Q}$, and we have checked that f is separable, the extension L is Galois over $\mathbf{Q}$. □

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

Problem 2 (7 points)**.** *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) (3 points) 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) Let $G = \mathsf{Gal}(L/\mathbf{Q})$. Every automorphism $g \in G$ of L must take α to a root of f and ζ to a primitive 11th root of unity, and every automorphism is determined by its values on $\{\alpha, \zeta\}$. This gives $11 \cdot 10$ possible automorphisms. Since $L/\mathbf{Q}$ is Galois, we have $|G| = [L : \mathbf{Q}] = 110$, so every possibility described actually gives an automorphism.

We want a generator of $(\mathbf{Z}/11)^\times = \mathsf{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$, so that sending ζ to this power and fixing α will give an automorphism of order 10. Since $2^{10/2} = 32 \not\equiv 1 \pmod{11}$ and $2^{10/5} = 4 \not\equiv 1 \pmod{11}$, one has that 2 is a generator of $(\mathbf{Z}/11)^\times$ (also called a primitive root mod 11). So setting $\sigma(\zeta) = \zeta^2$ and $\sigma(\alpha) = \alpha$ defines an automorphism $\sigma \in G$ of order 10 which fixes α.

Define $\tau \in G$ by $\tau(\alpha) = \zeta\alpha$ and $\tau(\zeta) = \zeta$. Then τ has order 11. Since σ, τ have relatively prime order, together they generate a group of order at least the product of their orders, hence they generate all of G.

Let $N = \langle\tau\rangle$. Then N is an 11-Sylow of G and N is normal in G by Sylow's theorem. Thus $\sigma\tau\sigma^{-1} = \tau^j$ for some j. We compute that $j = 2$:

$$\sigma\tau\sigma^{-1}(\alpha) = \sigma\tau(\alpha) = \sigma(\zeta\alpha) = \sigma(\zeta)\sigma(\alpha) = \zeta^2\alpha.$$

Hence

$$\sigma\tau\sigma^{-1} = \tau^2$$

and

$$G = \langle\sigma,\ \tau \mid \sigma^{10} = \tau^{11} = 1,\ \sigma\tau\sigma^{-1} = \tau^2\rangle$$

describes G by generators and relations (also known as a presentation of G).

(b) The normal subgroup N is solvable since it is cyclic. Let $H = \langle\sigma\rangle$. Then $G/N \cong H$ is cyclic, so it is solvable too. If G is a group with a normal subgroup N, then G is solvable if and only if both N and G/N are solvable. So G is solvable.

Alternatively, f is solvable by radicals because each of its roots is obtained, by definition, by a simple radical extension. Hence G is solvable by the dictionary between solvable Galois groups and polynomials solvable by radicals.

(c) First we note that $\mathbf{Q}(\zeta) = L^N$ is the unique intermediate field $\mathbf{Q} \subset K \subset L$ such that $K/\mathbf{Q}$ has degree 10. By the Galois correspondence, an extension $K/\mathbf{Q}$ of degree 10 corresponds to a subgroup of G of index 10 i.e., of order 11. Such a subgroup is an 11-Sylow, hence equals N. So the uniqueness of K follows from the uniqueness of an 11-Sylow in G. We see that $\mathbf{Q}(\zeta)/\mathbf{Q}$ is Galois, bot directly as splitting field of $x^{11} - 1$ but also via the correspondence because N is normal in G.

A quadratic $F/\mathbf{Q}$ contained in L corresponds to a subgroup M of G of index 2. Then M contains a unique 11-Sylow because an 11-Sylow of M is an 11-Sylow of G, and we determined N is the unique 11-Sylow of G (Variant: apply Sylow's theorem to M). Hence N is also the unique 11-Sylow of M. Passing over to fixed fields, $N \subset M$ corresponds to

$$F = L^M \subset K = L^N.$$

Since $\mathsf{Gal}(K/\mathbf{Q}) \cong H$ is cyclic, it has a unique subgroup of index 2, which corresponds to the unique quadratic $F/\mathbf{Q}$ contained in K which is also the unique quadratic $F/\mathbf{Q}$ contained in L.

We have seen in class that $\mathbf{Q}(\sqrt{p^*})$ is the unique quadratic $F/\mathbf{Q}$ contained in $\mathbf{Q}(\mu_p)$, where p^* is p if $p \equiv 1 \pmod 4$ and $-p$ if $p \equiv 3 \pmod 4$. Since $11 \equiv 3 \pmod 4$, we conclude that $F = \mathbf{Q}(\sqrt{-11})$. $\square$

Problem 3 (6 points)**.** *On this problem, if you solve (b) you can cite it in (a). But (a) can also be done by different methods which you may find easier (so you might be able to do (a) even if you don't manage (b)).*

(a) (1 point) Show that a subgroup of S_5 containing a 5-cycle and a transposition is all of S_5.

(b) (2 point) Let p be a prime. Show that a subgroup of S_p containing a p-cycle and a transposition is all of S_p.

(c) (1 point) Prove or give a counterexample to the following statement: "For every integer $n \geq 2$, if a subgroup H of S_n contains an n-cycle and a transposition, then $H = S_n$".

(d) (2 point) Assume that $f \in \mathbf{Q}[x]$ is irreducible of degree 5, that f is solvable by radicals and that the discriminant of f is negative. What is the order of $\mathsf{Gal}(f)$?

Solution. (a) One way is to apply the solution to (b) below. Here is another way: Let P be a 5-Sylow of S_5. Computing the number of p-cycles in S_p, then the number of p-Sylows in S_p, we find as in Abstract Algebra that the normalizer $N_{S_5}(P)$ has order 20 and that it is generated by a 4-cycle and a generator of P. It follows that all the elements of order 2 in $N_{S_5}(P)$ are of type $(2,2)$, so that $N_{S_5}(P)$ contains no transposition. Therefore, if $H \subset S_5$ is a subgroup containing P and a transposition, then the order of H is > 20, since it is divisible by 2 and 5, and a group of order 10 or 20 has a normal 5-Sylow. Hence $H = S_5$.

(b) Let $\tau \in S_p$ be a transposition and let σ be a p-cycle. We have $g\langle\sigma,\tau\rangle g^{-1} = \langle g\sigma g^{-1}, g\tau g^{-1}\rangle$. So we may assume that $\sigma = (12\cdots p)$ (but we may not assume also that $\tau = (12)$, for we may not be able to conjugate σ and τ to these values *simultaneously*, even though we can achieve each conjugation separately). Let $\tau = (ab)$. Then

$$\sigma\tau\sigma^{-1} = (\sigma(a)\sigma(b)) = (a+1\ b+1),$$

where $a+1, b+1$ are interpreted $\pmod p$. The orbit of $\langle\sigma\rangle$ acting on τ has size p since p is prime and the size of the orbit divides the size of the group (orbit-stabilizer, Lagrange). The orbit consists of the p transpositions $(c\ d)$ satisfying $|c-d| \equiv |b-a| \pmod p$. Then every $c \in \mathbf{Z}/p$ appears in precisely 2 of these p transpositions, namely, $(c\ c+b-a)$ and $c\ c+a-b)$, where again $b-a$ and $a-b$ are $\pmod p$. Removing 1 of the p transpositions, say removing $(a\ b)$ we are left with $p-1$ transpositions; now all but two $c = a$ and $c = b$ still appear in 2 of the transpositions, while $c = a$ and $c = b$ only appear in one transposition.

We order the $p-1$ transpositions as follows: Put $(a\ (a+a-b))$ first, then the unique other transposition among the $p-1$ in which $a+a-b = 2a-b$ occurs and continue in this way, so that the jth and $j+1$ transpositions in our ordering share one member. The last transposition left will be $(b\ (b+b-a))$. Then our list is

$$(a\ 2a-b),\ (2a-b\ 3a-2b)\cdots(b\ 2b-a),$$

where $a-b$ is added to each component as we move one to the right, and adding $(p-1)(a-b) \pmod p$ is the same as subtracting $a-b \pmod p$.

Then conjugation by

$$g = \begin{pmatrix} 1 & 2 & 3 & \cdots & p-1 & p \\ a & 2a-b & 3a-2b & \cdots & 3b-2a & 2b-a \end{pmatrix}$$

simultaneously takes

$$(12),\ (23),\ \cdots,(p-1\ p)$$

to

$$(a\ 2a-b),\ (2a-b\ 3a-2b)\cdots(b\ 2b-a),$$

or equivalently g^{-1} conjugates

$$(a\ 2a-b),\ (2a-b\ 3a-2b)\cdots(b\ 2b-a),$$

to

$$(12),\ (23),\ \cdots,(p-1\ p)$$

So these two sets of $p-1$ transpositions generate subgroups of the same size. But we know from abstract algebra that

$$(12),\ (23),\ \cdots,(n-1\ n)$$

generates S_n for any n (prime or not), because we can write any transposition as a product of these 'elementary' ones. So the subgroup generated by σ,τ is S_p.

(c) Here is a counterexample for $n = 4$: Let $\tau = (13)$ and $\sigma = (1234)$. Then

$$\tau\sigma\tau^{-1} = (3214) = (1432) = \sigma^{-1},$$

so σ, τ generate a dihedral group of order 8 inside S_4 (so not all of S_4).

(d) We claim that $\mathsf{Gal}(f)$ is a Frobenius group F_{20} of order 20; in other words, $\mathsf{Gal}(f)$ is the normalizer of a 5-Sylow subgroup of S_5 (the unique 5-Sylow that $\mathsf{Gal}(f)$ contains). Since f is irreducible over a field of characteristic zero, f is separable. Since f is irreducible of prime degree $p = 5$, its Galois group contains a p-cycle. So $\mathsf{Gal}(f)$ contains a 5-cycle. Since f is solvable by radicals $\mathsf{Gal}(f)$ is solvable, so $\mathsf{Gal}(f)$ does not contain A_5 (as A_5 is non-abelian and simple). Since $\mathsf{Disc}(f) < 0$, the discriminant is not a square in $\mathbf{Q}$, so $\mathsf{Gal}(f)$ is not contained in A_5. Hence $\mathsf{Gal}(f)$ is neither $\mathbf{Z}/5$ nor dihedral D_{10} of order 10 (as in (a), an element of order 2 normalizing a 5-Sylow of S_5 is of type $(2, 2)$, hence even). The only option left among the transitive subgroups of S_5 is F_{20} of order 20. □

Problem 4 (4 points)**.**

(a) (1 points) Let $f(x) = x^n - x + b \in \mathbf{Z}[x]$ and let q be a prime divisor of b. Show that f is separable in $\mathbf{F}_q[x]$ if and only if q does not divide $n-1$.

(b) (3 points) Show that the Galois group $\mathsf{Gal}(f) \subset S_{13}$ of $f(x) = x^{13} - x + 385$ over $\mathbf{Q}$ contains a 13-cycle, as well as elements of cycle type

$$(2,2,2),\ (2,2,2,2),\ \text{and}\ (2,2,2,2,2)$$

(here e.g., $(2,2,2)$ means a product of three disjoint transpositions).

Solution. (a) The derivative of f is $f'(x) = nx^{n-1} - 1$. One has $f \equiv x^n - x \pmod{q}$ since $q|b$. Now $(f, f') \neq 1$ in $\mathbf{F}_q[x]$ if and only if $(f, xf') \neq (x)$, which is if and only $(xf' - f, f) \neq x$. But $xf' - f = (n-1)x^n$.

Alternatively, the formula for the discriminant of a trinomial $x^n + ax + b$ (covered in exercise session) gives that

$$\mathsf{Disc}(f) = (-1)^{n(n-1)/2}[(n^n)b^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n)],$$

so in our case (with $a = -1$ and $q|b$), one has

$$\mathsf{Disc}(f) \equiv \pm(n-1)^{n-1} \pmod{q}$$

so $\mathsf{Disc}(f) = 0$ in $\mathbf{F}_q$ if and only if q divides $n-1$.

(b) We use the method of reducing f modulo different primes p not dividing $\mathsf{Disc}(f)$ to find cycle types in $\mathsf{Gal}(f)$. Since f is an Artin-Schreier polynomial mod $p = 13$ (of the form $x^p - x + a$, $a \in \mathbf{F}_p^\times$), f is irreducible in $\mathbf{F}_{13}[x]$. So $\mathsf{Gal}(f)$ contains a 13-cycle.

Note that $385 = 5 \cdot 7 \cdot 11$. So we reduce mod $5, 7, 11$; by (a) f is separable mod these primes and reduces to $x^{13} - x = x(x^{12} - 1)$. We know that $x^n - 1$ is the product of all the cyclotomic polynomials $\Phi_d(x)$ over all divisors $d|n$. We have seen that $\Phi_d(x)$ factors mod p, for p not dividing d, as a product of $\varphi(d)/r$ irreducible factors, each of degree r, where r is the order of p mod d.

Note that every element $x \in (\mathbf{Z}/12)^\times$ satisfies $x^2 = 1$. For $p = 5$, we have $p \equiv 1 \pmod{4}$, but $p \not\equiv 1$ mod each of the divisors $3, 6, 12$. So p has order 1 mod $d = 4$, but order 2 mod $3, 6$ and 12. So f reduces mod 5 to a product of linear factors times $1 + 1 + 2 = 4$ irreducible quadratics (so the number of linear factors is 5, counting x, which also corresponds to the divisors $d = 1, 2, 4$ with multiplicities $1, 1, 2$, plus 1 for x). This gives an element of cycle type $(2,2,2,2)$ in $\mathsf{Gal}(f)$. Similarly, reduction mod 7 gives an element of type $(2,2,2)$ because $7 \equiv 1$ mod 3 and 6 but $\not\equiv 1$ mod 4 and 12. Finally, the reduction of f mod 11 factors as a product of 3 linear factors and 5 irreducible quadratics, giving an element of cycle type $(2,2,2,2,2)$. □

Problem 5 (8 points)**.** *Let ζ_n be a primitive nth root of unity in some extension of $\mathbf{Q}$.*

(a) (2 points) Find $m_{\zeta_7+\zeta_7^{-1},\mathbf{Q}}(x)$.

(b) (1 point) Is $\cos(2\pi/7)+5$ constructible by straightedge and compass?

(c) (2 points) Let p be a prime different from 7. Show that $m_{\zeta_7+\zeta_7^{-1},\mathbf{Q}}(x)$ is irreducible in $\mathbf{F}_p[x]$ if $p \not\equiv \pm 1 \pmod 7$ and that otherwise $m_{\zeta_7+\zeta_7^{-1},\mathbf{Q}}(x)$ splits completely in $\mathbf{F}_p[x]$.

(d) (2 points) Recall that 97 is prime. Let $\mathbf{F}_{97}^{\times,3}$ be the subgroup of cubes in $\mathbf{F}_{97}^{\times}$. Define

$$\alpha = \sum_{a \in \mathbf{F}_{97}^{\times,3}} \zeta_{97}^a.$$

Determine the degree of α over $\mathbf{Q}$.

(e) (1 points) Let α be the element defined in (d). Is α solvable by radicals? Justify your answer.

Solution. Let $\alpha = \zeta_7 + \zeta_7^{-1}$; this is the sum of all powers of ζ_7 which are cubes in $(\mathbf{Z}/7)^\times$. Let $\beta := \zeta_7^2 + \zeta_7^{-2}$ and $\gamma := \zeta_7^3 + \zeta_7^{-3}$. For $a \in (\mathbf{Z}/7)^\times$, define $\sigma_a \in \mathsf{Gal}(\mathbf{Q}(\zeta_7)/\mathbf{Q})$ by $\sigma_a : \zeta_7 \mapsto \zeta_7^a$. Then $\sigma_3(\alpha) = \gamma$ and $\sigma^2(\alpha) = \beta$, so α, β, γ are Galois conjugates. Moreover, they are fixed by the subgroup $\langle \sigma_{-1} \rangle$ of cubes. So α, β, γ satisfy the same irreducible polynomial of degree 3 over $\mathbf{Q}$.

Let $f(x) := m_{\zeta_7+\zeta_7^{-1}}(x)$. The x^2 term of f is

$$-(\alpha+\beta+\gamma) = -(\zeta_7 + \cdots + \zeta_7^6) = +1.$$

The constant term of f is $-\alpha\beta\gamma$; one can multiply out explicitly the 8 terms, but it is not necessary: The 8 terms will be of the form ζ^j, we know that the sum is rational as it is fixed by Galois, and the one and only way to write a rational number b in the basis $\zeta_7, \ldots, \zeta_7^6$ is to take all coefficients equal to $-b$. So the 8 terms must comprise precisely 2 which are $\zeta^7 = 1$ and six which make $\zeta_7 + \cdots + \zeta_7^6 = -1$. So the constant term is $-(2-1) = -1$. The coefficient of x is $\alpha\beta + \alpha\gamma + \beta\gamma$, a sum of 12 terms ζ^j, none of which is 1, so the sum is -2. Hence

$$f(x) = x^3 + x^2 - 2x - 1.$$

(b) Note that $\cos(2\pi/7)$ and $\cos(2\pi/7)+5$ generate the same extension of $\mathbf{Q}$ since they differ by a rational number; this extension is $\mathbf{Q}(\alpha)$ since $2\cos\theta = e^{i\theta} + e^{-i\theta}$. Hence $\cos(2\pi/7)+5$ is not constructible by straightedge and compass, since it has degree 3, which is not a power of 2, over $\mathbf{Q}$.

(c) One has $p \equiv \pm 1 \pmod 7$ if and only if p is (nonzero and) a cube mod 7. If p is not a cube mod 7, then the Frobenius $x \mapsto x^p$ maps α to β (resp. γ) and its square $x \mapsto x^{p^2}$ maps α to γ (resp. β) if $p \equiv \pm 2 \pmod 7$ (resp. $p \equiv \pm 3 \pmod 7$). So α, β, γ are again Galois conjugates and f is irreducible mod p.

Conversely,if p is a cube mod 7, then Frobenius fixes each of α, β, γ, so $\alpha, \beta, \gamma \in \mathbf{F}_p$, since we know the Galois group of a splitting field of f is a finite extension of $\mathbf{F}_p$, hence its Galois group is cyclic generated by Frobenius. So α, β, γ are fixed by Galois, hence lie in the base field.

Remarks: To make sense of $\alpha, \beta, \gamma \pmod p$ we have two options: (1) We can consider the ring $\mathbf{Z}[\zeta_7]$ and reduce modulo a maximal ideal containing p as explained in class, or (2) We can take a splitting field of $x^7 - 1$ over $\mathbf{F}_p$, take a primitive ζ_7 in there, form α, β, γ there and do the whole argument in that finite extension of $\mathbf{F}_p$ (and our objects will be those obtained by reduction mod p via (1)).

(d) The degree of α over $\mathbf{Q}$ is 3 because α is fixed by the subgroup of cubes (as in (a)) which has index 3, and if g is a generator of $\mathbf{F}_{97}^\times$, then $\alpha, g\alpha, g^2\alpha$ are all distinct, because $\zeta_{97}, \ldots, \zeta_{97}^{96}$ is a basis of $\mathbf{Q}(\zeta_{97})/\mathbf{Q}$. So $\mathsf{Gal}(\mathbf{Q}(\zeta_{97})/\mathbf{Q}(\alpha))$ is precisely the subgroup of cubes.

(e) Yes, α is solvable by radicals because $\mathbf{Q}(\alpha)/\mathbf{Q}$ is a cyclic extension, hence solvable (its Galois group is a quotient of the Galois group $\mathsf{Gal}(\mathbf{Q}(\zeta_{97})/\mathbf{Q}) \cong \mathbf{Z}/96$; hence $\mathsf{Gal}(\mathbf{Q}(\alpha)/\mathbf{Q}) \cong \mathbf{Z}/3$). □