# 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* $f(x) = x^{13} - 15 \in \mathbf{Q}[x]$.

(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 both $p = 3$ and $p = 5$. Hence $f$ is irreducible over $\mathbf{Q}$ by Gauss' Lemma.

(b) Let $\zeta$ be a primitive 13th root of unity and let $\alpha$ 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 $i \in \mathbf{Z}/13$. 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 $13x^{12}$, 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 $\beta$ be another root of $f$, distinct from $\alpha$. Then $\alpha/\beta$ is not 1 but is a root of $x^{13} - 1$; whence $\alpha/\beta$ is a primitive 13th root of unity. Any subfield of $L$ over which $f$ splits must contain $\alpha, \beta$, so it must also contain a primitive 13th root of unity, so it contains all 13th roots of unity, so it contains $L$.

(c) The degree of a composite is always at most the product of the degrees, so $[L : \mathbf{Q}] \leq [\mathbf{Q}(\zeta) : \mathbf{Q})][\mathbf{Q}(\alpha) : \mathbf{Q}] = 12 \cdot 13 = 156$. Since $12, 13$ are relatively prime, we have equality by the multiplicativity of degrees in towers. So $[L : \mathbf{Q}] = 12 \cdot 13 = 156$.

(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 $\mathbf{Q}$. $\square$

*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* $\mathrm{Gal}(L/\mathbf{Q})$.

*(b) (2 points) Show that* $\mathrm{Gal}(L/\mathbf{Q})$ *is solvable.*

*(c) (2 points) Show that there is a unique extension $K/\mathbf{Q}$ of degree 12 which is contained in $L$.*

*(d) (2 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 $G = \mathrm{Gal}(L/\mathbf{Q})$. Every automorphism $g \in G$ of $L$ must take $\alpha$ to a root of $f$ and $\zeta$ to a primitive 13th root of unity, and every automorphism is determined by its values on $\{\alpha, \zeta\}$ . This gives $13 \cdot 12$ possible automorphisms. Since $L/\mathbf{Q}$ is Galois, we have $|G| = [L : \mathbf{Q}] = 156$, so every possibility described actually gives an automorphism.

We want a generator of $(\mathbf{Z}/13)^\times = \mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$, so that sending $\zeta$ to this power and fixing $\alpha$ will give an automorphism of order 12. Since $2^{12/2} = 64 \not\equiv 1 \pmod{13}$ and $2^{12/4} = 8 \not\equiv 1 \pmod{13}$, one has that 2 is a generator of $(\mathbf{Z}/13)^\times$ (also called a primitive root mod 13). So setting $\sigma(\zeta) = \zeta^2$ and $\sigma(\alpha) = \alpha$ defines an automorphism $\sigma \in G$ of order 12 which fixes $\alpha$.

Define $\tau \in G$ by $\tau(\alpha) = \zeta\alpha$ and $\tau(\zeta) = \zeta$. Then $\tau$ has order 13. Since $\sigma, \tau$ 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 a 13-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

$$G = \langle \sigma,\ \tau \mid \sigma^{12} = \tau^{13} = 1,\ \sigma\tau\sigma^{-1} = \tau^2 \rangle$$

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) By the Galois correspondence, an extension $K/\mathbf{Q}$ of degree 12 corresponds to a subgroup of $G$ of index 12 i.e., of order 13. Such a subgroup is a 13-Sylow, hence equals $N$. So the uniqueness of $K$ follows from the uniqueness of a 13-Sylow in $G$.

(d) A quadratic $F/\mathbf{Q}$ contained in $L$ corresponds to a subgroup $M$ of $G$ of index 2. Then $M$ contains a unique 13-Sylow by Sylow's theorem, hence $N$ is the unique 13-Sylow of $M$ as well. Passing over to fixed fields, $N \subset M$ says that

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

Since $\mathrm{Gal}(K/\mathbf{Q}) \cong H$ 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 $13 \equiv 1 \pmod 4$, we conclude that $F = \mathbf{Q}(\sqrt{13})$. $\square$

**Problem 3.** *Let $\Phi_{24}(x) \in \mathbf{Z}[x]$ be the cyclotomic polynomial of primitive 24th roots of unity. Let $\zeta$ be a root of $\Phi_{24}(x)$ in some finite extension of $\mathbf{Q}$.*

*(a) (2 points) Show that for every prime $p$, the reduction of $\Phi_{24}(x)$ modulo $p$ is reducible in $\mathbf{F}_p[x]$.*
*(b) (2 points) Is the regular 24-gon constructible by straightedge and compass? Justify your answer.*
*(c) (2 points) Show that there are precisely 7 quadratic extensions of $\mathbf{Q}$ contained in $\mathbf{Q}(\zeta)$.*

*Solution.* (a) We have seen that, given $p$ not dividing $n$, the cyclotomic polynomial $\Phi_n(x)$ factors in $\mathbf{F}_p[x]$ as a product of $\varphi(n)/d$ polynomials of degree $d$, where $d$ is the order of $p$ in $(\mathbf{Z}/n)^\times$.

One has $\varphi(24) = \varphi(8)\varphi(3) = 4 \cdot 2 = 8$. By contrast, given $x \in (\mathbf{Z}/24)^\times$, one has $x^2 = 1$ (e.g., use the Chinese Remainder Theorem). Hence $\Phi_{24}(x)$ is reducible modulo all primes $p$ not dividing 24.

Finally $x^{24} - 1 = (x^3 - 1)^8$ in $\mathbf{F}_2[x]$ and $x^{24} - 1 = (x^8 - 1)^3$ in $\mathbf{F}_3[x]$.

(b) The regular 24-gon is constructible by straightedge and compass because 24 is a power of 2 times a Fermat prime.

(c) We have $\mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q}) = (\mathbf{Z}/24)^\times \cong (\mathbf{Z}/2)^3$. Quotients of $(\mathbf{Z}/2)^3$ of order 2 are the same as quotient lines of the $\mathbf{F}_2$-vector space $\mathbf{F}_2^3$. Quotient lines are in duality with one-dimensional subspaces. The number of one dimensional subspaces in an $\mathbf{F}_p$-vector space of dimension $n$ is $(p^n - 1)/(p-1)$. But we can also compute directly that in an $\mathbf{F}_p$-vector space of dimension 3, the number of two-dimensional subspaces is

$$\frac{(p^3-1)(p^3-p)}{(p^2-1)(p^2-p)} = p^2 + p + 1 = \frac{p^3-1}{p-1}.$$

For $p = 2$, this gives 7 quotient lines. By the Galois correspondence, the 7 quotients of order 2 correspond to 7 quadratic $F/\mathbf{Q}$ contained in $\mathbf{Q}(\zeta)$. □

**Problem 4.** *Let $f(x) = x^4 + ax^2 + b \in \mathbf{Q}[x]$.*

*(a) (2 points) Show that the roots of $f$ in a splitting field have the form $\pm\alpha, \pm\beta$ and that $(\alpha\beta)^2 \in \mathbf{Q}$.*

*(b) (2 points) Show that $f(x)$ is irreducible over $\mathbf{Q}$ if and only if none of $\alpha^2, \alpha+\beta$ and $\alpha-\beta$ lie in $\mathbf{Q}$.*

*(c) (2 points) Assume $f$ is irreducible. Show that the Galois group of $f$ has order 4 or 8.*

*(d) (2 points) Assume $f$ is irreducible. Show that the Galois group of $f$ is the Klein 4-group $\mathbf{Z}/2 \times \mathbf{Z}/2$ if and only if $\alpha\beta \in \mathbf{Q}$.*

*Solution.* Note that this problem is adapted from [1, §14.6 Problem 13].

(a) One option is to solve explicitly by radicals using the quadratic formula, since $f$ is quadratic in the variable $y = x^2$.

Without computation: If $\gamma$ is a root of $f$ in an extension, then so is $-\gamma$, because $f$ is even (only has even degree terms). It remains to show that $(\alpha\beta)^2$ is rational.

If either $\alpha$ or $\beta$ is zero, then $(\alpha\beta)^2 = 0$ is rational. So we may assume $\alpha\beta \neq 0$. If $f$ is not separable, the (a) implies that $f(x) = (x-\alpha)^2(x+\alpha)^2 = (x^2-\alpha^2)^2$ and $b = \alpha^4 = (\alpha\beta)^2$ so $(\alpha\beta)^2 \in \mathbf{Q}$.

Finally, suppose $f$ is separable. If $\sigma \in \mathrm{Gal}(f)$, then $\sigma$ is determined by its action on $\alpha, \beta$ and $\sigma(\alpha\beta) = \pm\alpha\beta$. Hence $\mathrm{Gal}(f)$ fixes $(\alpha\beta)^2$, so $(\alpha\beta)^2 \in \mathbf{Q}$.

(b) By (a), $f$ has no irreducible factor of degree 3 over $\mathbf{Q}$. So $f$ is reducible if and only if $f$ has a degree 2 factor over $\mathbf{Q}$ (which may be reducible), if and only if

$$g(x) = (x-\gamma)(x-\delta) = x^2 - (\gamma+\delta)x + \gamma\delta \in \mathbf{Q}[x]$$

for two roots $\gamma, \delta \in \{\pm\alpha, \pm\beta\}$ of $f$.

In particular, if $f$ is reducible, then $\gamma + \delta \in \mathbf{Q}$ for some choice of $\gamma, \delta$ and $\gamma + \delta$ ranges over $-\alpha^2, \pm(\alpha+\beta), \pm(\alpha-\beta), -\beta^2$. So one of these is in $\mathbf{Q}$ which implies that one of $\alpha^2, \alpha+\beta, \alpha-\beta$ is in $\mathbf{Q}$, because $-\beta^2 \in \mathbf{Q}$ implies $\alpha^2 \in \mathbf{Q}$ by $(\alpha\beta)^2 \in \mathbf{Q}$ of (a).

Conversely, we may assume $f$ is separable; else $f$ is reducible because we are in characteristic zero. If $\alpha^2 \in \mathbf{Q}$, then $g(x) = x^2 - \alpha^2 \in \mathbf{Q}[x]$ is a quadratic factor. If $\alpha + \beta \in \mathbf{Q}$, then we claim that $g(x) = x^2 - (\alpha+\beta)x + \alpha\beta \in \mathbf{Q}[x]$ is a quadratic factor over $\mathbf{Q}$. To see this, it suffices to show that $\alpha + \beta \in \mathbf{Q}$ implies $\alpha\beta \in \mathbf{Q}$. But $\alpha + \beta \in \mathbf{Q}$ If $\alpha + \beta \in \mathbf{Q}$, then $\alpha + \beta$ is fixed by $\mathrm{Gal}(f)$ (here we use that $f$ is separable), so $\sigma\alpha, \sigma\beta \in \{\alpha, \beta\}$ and the two values are distinct, so $\sigma(\alpha\beta) = \alpha\beta$ for all $\sigma \in \mathrm{Gal}(f)$, whence $\alpha\beta \in \mathbf{Q}$.

The case where $\alpha - \beta \in \mathbf{Q}$ is analogous, with $g(x) = x^2 - (\alpha-\beta)x - \alpha\beta$ in place of $g(x) = x^2 - (\alpha+\beta)x + \alpha\beta$.

(c) Let $G = \mathrm{Gal}(f)$. Since an automorphism satisfies $\sigma(-\alpha) = -\sigma(\alpha)$, a $\sigma \in G$ is determined by its values on $\alpha, \beta$. There are 4 choices $\pm\alpha, \pm\beta$ for $\sigma(\alpha)$, and then both $\pm\sigma(\alpha)$ are excluded as choices for $\sigma(\beta)$, so there are at most 2 choices remaining for $\sigma(\beta)$. This shows $|G| \leq 8$. On the other hand, given $f$ irreducible of degree $n$, we know that $\mathrm{Gal}(f)$ acts transitively on the set of its $n$ distinct roots in a splitting field, hence $n$ divides $|\mathrm{Gal}(f)|$ by the Orbit-Stabilizer theorem. So 4 divides $|G|$ in our case, whence $|G| = 4$ or 8.

(d) Assume $\alpha\beta \in \mathbf{Q}$. Then every $\sigma \in \mathrm{Gal}(f)$ is uniquely determined by its action on $\alpha$, so $\mathrm{Gal}(f)$ has order 4 (the order is divisible by 4 by irreducibility of $f$ as in (c)). For every $\gamma \in \{\pm\alpha, \pm\beta\}$ there exists a unique $\sigma \in \mathrm{Gal}(f)$ mapping $\alpha$ to $\gamma$. For each of these choices, one sees that $\sigma^2 = 1$. For example, if $\sigma(\alpha) = \beta$, then $\sigma(\beta) = \alpha$ because $\sigma(\alpha\beta) = \alpha\beta$ by virtue of $\alpha\beta \in \mathbf{Q}$. Since $\mathrm{Gal}(f)$ has order 4 it is abelian, and since every element satisfies $\sigma^2 = 1$, we conclude $\mathrm{Gal}(f) \cong \mathbf{Z}/2 \times \mathbf{Z}/2$. □

**Problem 5.**

*(a) (1 point) Show that* $x^3 - 2$ *divides* $x^{343} - x$ *in* $\mathbf{F}_7[x]$.

*(b) (2 points) Show that the* $8$*th cyclotomic polynomial* $\Phi_8(x) = x^4 + 1$ *divides* $x^{p^2} - x$ *in* $\mathbf{F}_p[x]$ *for every odd prime* $p$.

*Solution.* (a) We know that $x^{p^n} - x$ factors over $\mathbf{F}_p$ as a product of all the irreducible polynomials in $\mathbf{F}_p[x]$ whose degree divides $n$. Since $2^3 \equiv 1 \pmod 7$, 2 cannot be a cube mod 7 (or check directly that 2 is not a cube mod 7). Since the degree of $x^3 - 2$ is at most 3 and it doesn't have a root in $\mathbf{F}_7$, it is irreducible over $\mathbf{F}_7$. Therefore $x^3 - 2$ divides $x^{7^3} - x$ in $\mathbf{F}_7[x]$.

(b) We know that, for $p$ not dividing $n$, the cyclotomic polynomial $\Phi_n(x)$ factors in $\mathbf{F}_p[x]$ as a product $\varphi(n)/d$ irreducible polynomials of degree $d$, where $d$ is the order of $p$ in $(\mathbf{Z}/n)^{\times}$. Since $(\mathbf{Z}/8)^{\times} \cong \mathbf{Z}/2 \times \mathbf{Z}/2$, every element in it has order dividing 2 and we conclude that $x^4 + 1$ divides $x^{p^2} - 1$ for every odd prime $p$. □

## References

[1] D. Dummit and R. Foote. *Abstract Algebra*. John Wiley and Sons, 3 edition, 2003.