MATH 3030, Abstract Algebra

Winter 2012

Toby Kenney

Sample Final Examination

This practice exam deliberately has more questions than the real exam. Some of the theoretical questions are directly from the notes, and some are new, requiring a little thought. The questions from the notes are intended to provide a complete list of theorems from the last part of the course that you might be asked to prove. These questions deliberately focus on the part of the course after the midterm, because there are already a number of practice questions available on the material before the midterm.

Basic Questions

1. *Which of the following pairs of numbers are conjugate over $\mathbb{Q}$?*

   (a) $\sqrt{3}$ and $\sqrt{3}i$

   These are not conjugate, because $\mathrm{Irr}(\sqrt{3},\mathbb{Q}) = x^2-3$, and $\mathrm{Irr}(\sqrt{3}i,\mathbb{Q}) = x^2+3$.

   (b) $\sqrt{2}+\sqrt{3}$ and $\sqrt{2}-\sqrt{3}$

   These are conjugate, because $(\sqrt{2}+\sqrt{3})^2 = 5+2\sqrt{6}$, so $\mathrm{Irr}(\sqrt{2}+\sqrt{3},\mathbb{Q}) = x^4-10x^2+1$, which has $\sqrt{2}-\sqrt{3}$ as a zero.

   (c) $\sqrt[5]{3}$ and $-\sqrt[5]{3}$.

   These are not conjugate, because $\mathrm{Irr}(\sqrt[5]{3},\mathbb{Q}) = x^5-3$, but $\mathrm{Irr}(-\sqrt[5]{3},\mathbb{Q}) = x^5+3$

2. *Which of the following pairs of numbers are conjugate over $\mathbb{Q}(\sqrt{2})$?*

   (a) $\sqrt[3]{3}$ and $\sqrt[3]{3}\left(-\frac{1}{2}+\frac{\sqrt{3}}{2}i\right)$

   These are conjugate over $\mathbb{Q}(\sqrt{2})$, since they both have irreducible polynomial x^3-3.

   (b) $\sqrt[4]{2}$ and $\sqrt[4]{2}i$

   These are not conjugate over $\mathbb{Q}(\sqrt{2})$, since $\mathrm{Irr}(\sqrt[4]{2},\mathbb{Q}(\sqrt{2})) = x^2-\sqrt{2}$, which does not have $\sqrt[4]{2}i$ as a zero.

3. *In $\mathbb{Q}(\sqrt[4]{3},i)$, what is the fixed field of the automorphism σ which leaves $\mathbb{Q}$ fixed, and sends $\sqrt[4]{3}$ to $-\sqrt[4]{3}$ and sends i to $-i$.*

   We know that $\mathbb{Q}(\sqrt[4]{3},i)$ is a normal extension of $\mathbb{Q}$. The automorphism σ has order 2, so it generates a subgroup of index 4 of $G(\mathbb{Q}(\sqrt[4]{3},i)/mathbbQ)$. Therefore, the fixed field has degree 4 over $\mathbb{Q}$. We see that $\sqrt[4]{3}i$ is left fixed by σ, but $[\mathbb{Q}(\sqrt[4]{3}i):\mathbb{Q}] = 4$, so $\mathbb{Q}(\sqrt[4]{3}i)$ is the fixed field of σ.

4. *Let α be a zero of x^4+3 in GF(5^4).*

   (a) Let σ_5 be the Frobenius automorphism. Compute ${\sigma_5}^2(\alpha)$ [Give your answer in the basis $\{1,\alpha,\alpha^2,\alpha^3\}$.]

   Since α is a zero of x^4+3, we have $\alpha^4=3$. Therefore, $\sigma_5(\alpha)=3\alpha$ and ${\sigma_5}^2(\alpha)=4\alpha$.

   (b) What is the fixed field of ${\sigma_5}^2$?

   We know that the Galois group of GF(5^4) is cyclic of order 4 generated by σ_5, so the subgroup generated by ${\sigma_5}^2$ has index 2. Therefore, the fixed field of ${\sigma_5}^2$ is GF(5^2), which consists of the zeros of $x^{25}-x$. We see that $\alpha^{16}=1$, so $(\alpha^2)^{24}=1$, so the fixed field is $\mathbb{Z}_3(\alpha^2)$.

   Alternatively: We know that ${\sigma_5}^2(\alpha)=4\alpha$ and so ${\sigma_5}^2(\alpha^2)=(4\alpha)^2=\alpha^2$, so the fixed field is $\mathbb{Z}_3(\alpha^2)$.

5. *Find an element α such that $\mathbb{Q}(\sqrt{2+\sqrt{3}},\sqrt{3+\sqrt{5}})=\mathbb{Q}(\alpha)$ [Hint: to calculate differences between conjugates, try squaring the difference.]*

   We can choose $\alpha=\sqrt{2+\sqrt{3}}+a\sqrt{3+\sqrt{5}}$ for any a which is not equal to $\frac{\beta_i-\beta}{\gamma_j-\gamma}$ for any conjugates β_i of $\beta=\sqrt{2+\sqrt{3}}$ and γ_j of $\gamma=\sqrt{3+\sqrt{5}}$. The conjugates of β are $-\sqrt{2+\sqrt{3}}$, $\sqrt{2-\sqrt{3}}$ and $-\sqrt{2-\sqrt{3}}$, and the conjugates of γ are $-\sqrt{3+\sqrt{5}}$, $\sqrt{3-\sqrt{5}}$, $-\sqrt{3-\sqrt{5}}$. We observe that $(\sqrt{2+\sqrt{3}}-\sqrt{2-\sqrt{3}})^2=2$, $(\sqrt{2+\sqrt{3}}+\sqrt{2-\sqrt{3}})^2=6$, while $(\sqrt{3+\sqrt{5}}-\sqrt{3-\sqrt{5}})^2=2$, $(\sqrt{3+\sqrt{5}}+\sqrt{3-\sqrt{5}})^2=10$ [other conjugates produce differences not in the intersection of the fields]. This means we must choose $a\neq 1,3,0.2,0.6$. For example, we can choose $\alpha=2$, so $\alpha=\sqrt{2+\sqrt{3}}+2\sqrt{3+\sqrt{5}}$ works.

6. *Find a basis for the splitting field of x^4-3 over $\mathbb{Q}$.*

   The zeros of x^4-3 are $\sqrt[4]{3}$, $\sqrt[4]{3}i$, $-\sqrt[4]{3}$ and $-\sqrt[4]{3}i$. The splitting field is therefore $\mathbb{Q}(\sqrt[4]{3},i)$. One basis is $\{1,i,\sqrt[4]{3},\sqrt[4]{3}i,\sqrt{3},\sqrt{3}i,\sqrt[4]{27},\sqrt[4]{27}i\}$.

7. *Let f be an irreducible polynomial of degree 4 over a field F. Let K be the splitting field of f over F. Let the zeros of f be α, β, γ and δ. What is the orbit of $\alpha\beta\gamma+\delta$ under $G(K/F)$.*

   The automorphisms in $G(K/F)$ permute α, β, γ and δ. The orbit of $\alpha\beta\gamma+\delta$ is therefore $\{\alpha\beta\delta+\gamma,\alpha\gamma\delta+\beta,\beta\gamma\delta+\alpha\}$. [It is the whole of this set because $G(K/F)$ is a transitive permutation group on α, β, γ and δ.]

8. *Write $\frac{a}{b}+\frac{b}{a}+\frac{a}{c}+\frac{c}{a}+\frac{a}{d}+\frac{d}{a}+\frac{b}{c}+\frac{c}{b}+\frac{b}{d}+\frac{d}{b}+\frac{c}{d}+\frac{d}{c}$ as a rational function in the elementary symmetric functions $a+b+c+d$, $ab+ac+ad+bc+bd+cd$, $abc+abd+acd+bcd$ and $abcd$.*

   First we multiply through by $abcd$ to get $a^2cd+b^2cd+a^2bd+c^2bd+a^2bc+d^2bc+b^2ad+c^2ad+b^2ac+d^2ac+c^2ab+d^2ab=(a+b+c+d)(abc+abd+acd+bcd)-4abcd$. Therefore, the expression is $\frac{s_1s_3}{s_4}-4$.

9. *How many extension fields of $\mathbb{Q}$ are contained in the splitting field of $f(x) = x^4 - 7$?*

   By Eisenstein's criterion, f is irreducible. The splitting field is $\mathbb{Q}(\sqrt[4]{7}, i)$. The zeros of f are $\pm\sqrt[4]{7}$ and $\pm\sqrt[4]{7}i$. Any automorphism of the splitting field must preserve these two opposite pairs that sum to zero, so the Galois group is D_4. Extension fields contained in the splitting field are in one-to-one correspondence with subgroups of D_4. There are 10 subgroups of D_4 (including the trivial and improper subgroups), so there are 10 extension fields contained in the splitting field of f (including the splitting field itself, and $\mathbb{Q}$).

10. *(a) Is the regular 36-gon constructible?*

    No because 36 is divisible by 3^2.

    (b) Is the regular 60-gon constructible?

    Yes, since $60 = 2^2 \times 3 \times 5$, and 3 and 5 are both Fermat primes.

11. *Find $\Phi_{26}(x)$ over $\mathbb{Q}$.*

    We know that $x^{26} - 1 = (x^{13} - 1)(x^{13} + 1) = (x^{13} - 1)(x + 1)(x^{12} - x^{11} + x^{10} - x^9 + x^8 - x^7 + x^6 - x^5 + x^4 - x^3 + x^2 - x + 1)$, and that $\phi(26) = 12$, so $\Phi_{26}(x) = x^{12} - x^{11} + x^{10} - x^9 + x^8 - x^7 + x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$.

bonus *Is $f(x) = x^5 - 15x^4 + 90x^3 - 270x^2 + 405x - 245$ solvable by radicals over $\mathbb{Q}$?*

Yes. $f(x) = (x-3)^5 - 2$, so the zeros are $3 + \zeta^n \sqrt[5]{2}$, where ζ is a primitive fifth root of unity.

12. *Is $f(x) = x^5 + x^3 + 2x + 3$ solvable by radicals over $\mathbb{Z}_7$?*

    Yes — any finite field consists of zeros of $x^q - x$, so all non-zero elements are zeros of $x^{q-1} - 1$, so it is a cyclotomic extension of the base field, so it is solvable by radicals.

13. *Let α be a zero of $x^3 + 2x^2 + x + 1$ over $\mathbb{Z}_3$. What are the conjugates of α over $\mathbb{Z}_3$.*

    By long division, $x^3 + 2x^2 + x + 1 = (x - \alpha)(x^2 + (\alpha + 2)x + (\alpha^2 + 2\alpha + 1))$, so the other zeros are the zeros of $x^2 + (\alpha + 2)x + (\alpha^2 + 2\alpha + 1)$, which by the quadratic formula are $(\alpha + 2) \pm \sqrt{2\alpha}$. We know that $\alpha^{26} = 1$, and if 2α is to be a square, then we must have $\alpha^{13} = 2$, so that $\sqrt{2\alpha} = \alpha^7$. We then compute $\alpha^6 = \alpha^4 + \alpha^3 + 2\alpha^2 + 2\alpha + 1 = 2\alpha^3 + \alpha^2 + \alpha + 1 = 2\alpha + 2$, so $\alpha^7 = 2\alpha^2 + 2\alpha$. We check that the square of this is indeed 2α. This gives that the two conjugates of α are $\alpha + 2 \pm (\alpha^2 + \alpha)$, which gives $\alpha^2 + 2\alpha + 2$ and $2\alpha^2 + 2$.

14. *What are the conjugates of $\sqrt{\sqrt{2} + 1}$ over $\mathbb{Q}$?*

    We see that $\sqrt{\sqrt{2} + 1}$ is a zero of $x^4 - 2x^2 - 1$ over $\mathbb{Q}$. The other zeros are $-\sqrt{\sqrt{2} + 1}$, $\sqrt{\sqrt{2} - 1}i$ and $-\sqrt{\sqrt{2} - 1}i$, so these are the conjugates of $\sqrt{\sqrt{2} + 1}$.

15. *What is the degree of the splitting field of $x^3 + 2x^2 + 6x - 2$ over $\mathbb{Q}$?*

Let the zeros of x^3+2x^2+6x-2 be α, β and γ. We have that $s_1 = \alpha+\beta+\gamma = -2$, while $s_2 = \alpha\beta + \alpha\gamma + \beta\gamma = 6$, so $\alpha^2 + \beta^2 + \gamma^2 = {s_1}^2 - 2s_2 = -8$. Since this is negative, the polynomial must have complex zeros, so the group of the splitting field must include complex conjugation, which has order 2, so it must be the whole of S_3. Therefore, the degree of the splitting field over $\mathbb{Q}$ is 6.

Theoretical Questions

Results from Notes

16. *Show that if α and β are elements of $\overline{F}$, show that there is an isomorphism $\sigma : F(\alpha) \longrightarrow F(\beta)$ such that $\sigma(a) = a$ for all $a \in F$ and $\sigma(\alpha) = \beta$, if and only if α and β are conjugate over F.*

Suppose the irreducible polynomial f for α has degree n over F. Since f has coefficients in F, we know that $f(\sigma(\alpha)) = \sigma(f(\alpha)) = \sigma(0) = 0$, so $\sigma(\alpha)$ must be conjugate to α. On the other hand, suppose α' is another zero of f. In this case $F(\alpha)$ and $F(\alpha')$ are both isomorphic to $F[x]/\langle f\rangle$, since we know that $\langle f\rangle$ is the kernel of the evaluation homomorphism at α and the evaluation homomorphism at α'. It is easy to see that the composite of one homomorphism with the inverse of the other gives an isomorphism $F(\alpha) \longrightarrow F(\alpha')$.

17. *Show that the set of elements of a field E left fixed by a set S of automorphisms of E is a subfield of E.*

Let F be the set of elements left fixed by all automorphisms in S. We need to show that F is closed under addition, multiplication, additive and multiplicative inverses. We already know that 0 and 1 are fixed by all automorphisms, as are all elements in the prime field so F must contain the prime field of E. F is closed under addition and multiplication, since if σ leaves α and β fixed then $\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)$ and $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta) = \alpha\beta$. F is closed under additive inverses because these are just multiplication by -1. Finally we know that $\sigma(\alpha^{-1}) = \sigma(\alpha)^{-1} = \alpha^{-1}$, so F is closed under multiplicative inverses. Thus F is a subfield of E.

18. *Let E be a field, and let F be a subfield of E. Show*

(a) the set of automorphisms of E forms a group under function composition.

We know that function composition is associative, so we just need to show that the composite of two automorphisms is an automorphism, the identity function is an automorphism and the inverse of an automorphism is an automorphism. These properties are clearly true for bijections, so we just need to show the necessary homomorphism properties. If ι is the identity

function, then we know that $\iota(\alpha+\beta) = \alpha+\beta = \iota(\alpha)+\iota(\beta)$ and $\iota(\alpha\beta) = \alpha\beta = \iota(\alpha)\iota(\beta)$. If σ is an automorphism of E, then $\sigma(\sigma^{-1}(\alpha)+\sigma^{-1}(\beta)) = \sigma(\sigma^{-1}(\alpha))+\sigma(\sigma^{-1}(\beta)) = \alpha+\beta$, so $\sigma^{-1}(\alpha+\beta) = \sigma^{-1}(\alpha)+\sigma^{-1}(\beta)$, and a similar argument for multiplication. Finally, we know that the composite of two homomorphisms is a homomorphism.

(b) the subset of automorphisms of E that leave F fixed is a subgroup of this group.

We need to show that if σ and τ leave F fixed, then σ^{-1} and $\sigma\tau$ leave F fixed, and also that the identity function leaves F fixed. For any α in F, we know that $\sigma(\alpha) = \alpha$, so $\sigma^{-1}(\alpha) = \alpha$, and $\sigma\tau(\alpha) = \sigma(\tau(\alpha)) = \sigma(\alpha) = \alpha$ as required. The identity obviously leaves F fixed.

19. *Let F be a finite field of characteristic p. Show that the map $\sigma_p : F \longrightarrow F$ given by $\sigma_p(x) = x^p$ is an automorphism of F.*

Clearly, $\sigma_p(\alpha\beta) = \sigma_p(\alpha)\sigma_p(\beta)$, and $\sigma_p(\alpha+\beta) = \sum_{i=0}^{p} \binom{p}{i}\alpha^i\beta^{p-i}$. However, in characteristic p, we have that $\binom{p}{i} = 0$ for any $i \neq 0, p$, so we get $\sigma_p(\alpha+\beta) = \alpha^p+\beta^p = \sigma_p(\alpha)+\sigma_p(\beta)$, so σ_p is a homomorphism. To show it is an isomorphism, we just need to show it has an inverse. However, if F has p^n elements, then all of them are zeros of $x^{p^n}-x$, so ${\sigma_p}^n(\alpha) = \alpha^{p^n} = \alpha$, so ${\sigma_p}^{n-1}$ is an inverse of σ_p, so it is an automorphism.

20. *Let E be a finite extension of F, and let $\sigma : F \longrightarrow F'$ be an isomorphism. Show that there is an isomorphism $\hat{\sigma} : E \longrightarrow E'$, where E' is a subfield of $\overline{F'}$ and such that for all $a \in F$, we have $\hat{\sigma}(a) = \sigma(a)$.*

Since E is a finite extension, of F, we have $E = F(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_1, \ldots, \alpha_n$. It is clear that if we can prove the result for simple extensions, then the whole result follows by induction, so let $E = F(\alpha)$. Let $f = \mathrm{Irr}(\alpha, F)$, and let $\sigma(f)$ be the polynomial in $F'[x]$ obtained by applying σ to each coefficient of f, that is if $f(x) = a_0 + \ldots + a_n x^n$, then $\sigma(f)(x) = \sigma(a_0)+\ldots+\sigma(a_n)x^n$. Let α' be a zero of $\sigma(f)$ in $\overline{F'}$. We can define a ring isomorphism $F[x] \longrightarrow F'[x]$ extending σ, in the obvious way. This clearly produces an isomorphism $F[x]/\langle f\rangle \longrightarrow F'[x]\langle\sigma(f)\rangle$, and composing with isomorphisms between these fields and $F(\alpha)$ and $F(\alpha')$ respectively, we get the isomorphism $\hat{\sigma}$.

21. *Show that if $F \leqslant E \leqslant K$ then $\{K : F\} = \{K : E\}\{E : F\}$.*

Given an isomorphism $\sigma : F \longrightarrow F'$, there are $\{E : F\}$ isomorphisms from E to a subfield of $\overline{F'}$ that extend σ. Each of these can be extended to $\{K : E\}$ different isomorphisms from K to a subfield of $\overline{F'}$. No two of these extensions can be the same, because they have different restrictions to E. This gives $\{K : E\}\{E : F\}$ isomorphisms from K to a subfield of $\overline{F'}$. Conversely, given an isomorphism from K to a subfield of $\overline{F'}$ that extends σ, its restriction to E is an isomorphism from E to a subfield of $\overline{F'}$, so it is one of the $\{K : E\}\{E : F\}$ isomorphisms we have already considered. Therefore, $\{K : F\} = \{K : E\}\{E : F\}$.

22. *Show that an algebraic extension E is a splitting field over F if and only if every automorphism σ of $\overline{F}$ that leaves F fixed restricts to an automorphism of E — that is, for all $x \in E$, $\sigma(x) \in E$.*

Let E be the splitting field of $\{f_i | i \in I\}$ over F, and let σ be an automorphism of $\overline{F}$ that leaves F fixed. Consider $\alpha \in E$. α is a polynomial in the zeros of the f_i, so it must be in the splitting field of some finite subset $\{f_{i_1}, \ldots, f_{i_n}\}$. Let K be the splitting field of this subset. We will show that $\sigma(\alpha) \in K$. We know that α is a polynomial in the zeros of $\{f_{i_1}, \ldots, f_{i_n}\}$, and since σ is an automorphism, $\sigma(\alpha)$ is a polynomial in the images of these zeros under σ. The images of these zeros are other zeros of the f_i, since they must be conjugates. Therefore, they are all in K, so $\sigma(\alpha) \in K$.

23. *Show that if E is a splitting field of finite degree over F, then $|G(E/F)| = \{E : F\}$.*

We need to show that any isomorphism $\sigma : E \xrightarrow{E} {}'$, where E' is a subfield of $\overline{F}$ is an automorphism of E. However, we know that σ can be extended to an automorphism of $\overline{F}$, and this restricts to an automorphism of E. This automorphism of E must be σ.

24. *Let $f \in F[x]$ be irreducible. Show that all zeros of f have the same multiplicity.*

Let α and β be zeros of f. Since f is irreducible, we have $\mathrm{Irr}(\alpha, F) = f = \mathrm{Irr}(\beta, F)$, so α and β are conjugate over F. Therefore, we have the conjugation isomorphism $\psi_{\alpha,\beta} : F(\alpha) \longrightarrow F(\beta)$. Now we know that in $F(\alpha)$, $f(x)$ factors as $(x - \alpha)^n g(x)$, where n is the multiplicity of α. The conjugation isomorphism then sends this to $(x - \beta)^n \psi_{\alpha,\beta}(g(x))$, so the multiplicity of β is at least n. By using the isomorphism $\psi_{\beta,\alpha}$, we get that the multiplicity of α is at least the multiplicity of β, so α and β have the same multiplicity.

25. *Show that if E is a finite extension of F, and K is a finite extension of E, then K is separable over F if and only if K is separable over E and E is separable over F.*

We know that $[K : F] = [K : E][E : F]$ and $\{K : F\} = \{K : E\}\{E : F\}$, so if K is separable over E and E is separable over F, then K is separable over F. Conversely, if K is separable over F, then we have $\{K : E\}\{E : F\} = [K : E][E : F]$, and since we have the inequalities $\{K : E\} \leqslant [K : E]$ and $\{E : F\} \leqslant [E : F]$, the only way to get $\{K : E\}\{E : F\} = [K : E][E : F]$ is if $\{K : E\} = [K : E]$ and $\{E : F\} = [E : F]$.

26. *Show that a field of characteristic zero is perfect. [You may assume that if $g^n \in F[x]$, then $g \in F[x]$ whenever F has characteristic zero.]*

Let F be a field of characteristic zero. We want to show that an irreducible polynomial in $F[x]$ cannot have a repeated zero. Let f be an irreducible

polynomial in $F[x]$. Without loss of generality, we can assume f is monic. Let the zeros of f in $\overline{F}$ be $\{\alpha_1, \ldots, \alpha_m\}$. We know that all zeros have the same multiplicity, because they are all conjugate over F. Let this multiplicity be n. We have that $f(x) = \Pi_{i=1}^{m}(x - \alpha_i)^n$, so if we define $g \in \overline{F}[x]$ by $g(x) = \Pi_{i=1}^{m}(x - \alpha_i)$, then we have $f = g^n \in F[x]$, so we have $g \in F[x]$. Since F is irreducible, this gives $g = f$, so all zeros of f have multiplicity 1. Therefore any finite extension of F is separable, so F is perfect.

27. *Show that any finite field is perfect.*

    Let F be a finite field with q elements, and let E be an extension of degree n over F. We know that all elements of E are zeros of $x^{q^n} - x$, so for any $\alpha \in E$, we have $\mathrm{Irr}(\alpha, F)$ divides $x^{q^n} - x$. Since $x^{q^n} - x$ has q^n zeros, they must all have multiplicity one, so all zeros of $\mathrm{Irr}(\alpha, F)$ must have multiplicity one, i.e. α is separable over F. Therefore, E is separable over F.

28. *Show that if E is a finite separable extension of an infinite field F, then $E = F(\alpha)$ for some α in E.*

    It is sufficient to prove the case when $E = F(\beta, \gamma)$ for some β and γ, since the general case then follows by induction. In this case, let $[F(\beta), F] = m$ and $[F(\beta, \gamma) : F(\beta)] = n$. We will choose $\alpha = \beta + a\gamma$ for some $a \in F$. The conjugates of this α over F are $\beta' + a\gamma'$ where β' is a conjugate of β over F and γ' is a zero of $\psi_{\beta,\beta'}(\mathrm{Irr}(\gamma, F(\beta)))$ over $F(\beta')$. If these conjugates are all different, then we see that the irreducible polynomial of α over F has degree mn, so that $F(\alpha) = F(\beta, \gamma)$. Therefore, we just need to choose a to make them different. That is, we can just choose a so that $\beta' + a\gamma' \neq \beta'' + a\gamma''$, i.e. $a \neq \frac{\beta' - \beta''}{\gamma' - \gamma''}$ for β' and β'' conjugates of β and γ' and γ'' conjugates of γ. Since β and γ have only finitely many conjugates over F, we have only ruled out a finite number of possibilities for a, so since F is infinite, we know that there is some suitable possibility for a.

29. *Show that for any subgroup H of $G(K/F)$, where K is a finite normal extension of F, we have $\lambda(K_H) = H$.*

    It is obvious that $H \leqslant \lambda(K_H)$ from the definitions, so we just need to prove the reverse inclusion. We can prove this by considering the order of the relevant subgroups. We will show that $[K : K_H] \leqslant |H|$, then we can deduce that $|\lambda(K_H)| = |H|$, and so the two subgroups are equal. We know that K is a finite normal extension of K_H, so $K = K_H(\alpha)$ for some $\alpha \in K$. Now consider the polynomial $f = \Pi_{\sigma \in H}(x - \sigma(\alpha))$. It is clear that this polynomial is left fixed by H, so it is in $K_H[x]$. We therefore have that $\mathrm{Irr}(\alpha, K_H)$ has degree at most $|H|$, but this is the degree $[K : K_H]$.

30. *Show that for any field $F \leqslant E \leqslant K$, where K is a finite normal extension of F, we have $K_{\lambda(E)} = E$.*

It is obvious that $E \leqslant K_{\lambda(E)}$, by the definitions. We therefore just need to show the reverse inclusion. We show that if $\alpha \notin E$, then α is not fixed by all automorphisms of K that fix E — that is, we need to construct an automorphism of K that fixes E but not α. Since $\alpha \notin E$, we have that $\mathrm{Irr}(\alpha, E)$ is a polynomial of degree more than 1. Since K is a separable extension of E, this means that $\mathrm{Irr}(\alpha, E)$ has more than one zero, so α has some conjugate α' over E. We now have the conjugation ismorphism $\psi_{\alpha,\alpha'} : E(\alpha) \longrightarrow E(\alpha')$. Since K is a splitting field, we can extend this to an automorphism σ of K that leaves E fixed, but sends α to α'. We have that $\sigma \in \lambda(E)$, but $\alpha \notin K_\sigma$, so we have shown $\alpha \notin K_{\lambda(E)}$ as required.

31. *Show that for any field $F \leqslant E \leqslant K$, where K is a finite normal extension of F, E is a normal extension of F if and only if $\lambda(E)$ is a normal subgroup of $G(K/F)$.*

Since K is separable over F, we know E must be, so E is a normal extension if and only if it is a splitting field over F, which happens if and only if any automorphism of K which leaves F fixed restricts to an automorphism of E.

Let $\sigma \in G(K/F)$ and suppose $\alpha \in E$ is such that $\sigma(\alpha) = \alpha' \notin E$. Since $\alpha' \notin E$, we can find some $\beta \neq \alpha'$ conjugate to α' over E. We can then find a conjugation isomorphism $\tau \in G(K/E)$ which sends α' to β. Now we have that $\sigma^{-1}\tau\sigma(\alpha) = \sigma^{-1}(\beta) \neq \alpha$, so that $\sigma^{-1}\tau\sigma \notin G(K/E)$, meaning $G(K/E)$ is not normal in $G(K/F)$. Conversely, if E is a normal extension of F, then any automorphism σ in $G(K/F)$ sends elements of E to elements of E, so for any $\tau \in G(K/E)$ and any $\alpha \in E$, we have $\sigma\tau\sigma^{-1}(\alpha) = \alpha$, so $\sigma\tau\sigma^{-1} \in G(K/E)$, and $G(K/E)$ is a normal subgroup of $G(K/F)$.

32. *Show that a symmetric function in $y_1, \ldots, y_n$ over F is a rational function of the elementary symmetric functions.*

Let the elementary symmetric functions be $s_1, \ldots, s_n$. Let S be the subfield of symmetric functions in $F(y_1, \ldots, y_n)$. We have a tower of extensions

$$\begin{array}{c} F(y_1, \ldots, y_n) \\ | \\ S \\ | \\ F(s_1, \ldots, s_n) \end{array}$$

We know that $F(y_1, \ldots, y_n)$ is a splitting field of $f(x) = x^n - s_1 x^{n-1} + \cdots + (-1)^n s_n$ over $F(s_1, \ldots, s_n)$, so it is a normal extension. Since f has degree n, we have $[F(y_1, \ldots, y_n) : F(s_1, \ldots, s_n)] \leqslant n!$. On the other

hand, by definition $S = F(y_1, \ldots, y_n)_{S_n}$, and we can see that the permutations of $\{y_1, \ldots, y_n\}$ all induce different automorphisms of $F(y_1, \ldots, y_n)$, so that $[F(y_1, \ldots, y_n) : S] \geqslant n!$. Thus, we have $n! \leqslant [F(y_1, \ldots, y_n) : S] \leqslant [F(y_1, \ldots, y_n) : F(s_1, \ldots, s_n)] \leqslant n!$. Thus all the inequalities are equalities, and $S = F(s_1, \ldots, s_n)$ as required.

33. *Show that the Galois group of the nth cyclotomic extension of $\mathbb{Q}$ is isomorphic to the group of integers relatively prime to n under multiplication modulo n.*

Let ζ be a primitive nth root of unity. The primitive nth roots of unity are ζ^m where m is coprime to n. An automorphism σ in $G(\mathbb{Q}(\zeta)/\mathbb{Q})$ is entirely determined by $\sigma(\zeta)$, which must be one of these primitive roots of unity. Let σ_i denote the automorphism with $\sigma_i(\zeta) = \zeta^i$. Then $\sigma_i(\sigma_j(\zeta)) = \sigma_i(\zeta^j) = (\sigma_i(\zeta))^j = (\zeta^i)^j = \zeta^{ij}$, so we get $\sigma_i\sigma_j = \sigma_{ij}$.

34. *Show that a regular n-gon is constructible if and only if all odd prime divisors of n are Fermat primes, and n is not divisible by the square of any odd prime.*

An angle of $\theta_n = \frac{360^\circ}{n}$ is constructible if and only if its cosine is constructible. Let $\zeta = \cos\theta_n + i\sin\theta_n$. Now since $\sin\theta_n = \sqrt{1 - \cos^2\theta_n}$, we have that $[\mathbb{Q}(\zeta, \cos\theta_n) : \mathbb{Q}(\theta_n)] \leqslant 2$, and $\cos\theta_n = \frac{\zeta + \zeta^{n-1}}{2} \in \mathbb{Q}(\zeta)$, so that $[\mathbb{Q}(\cos\theta_n) : \mathbb{Q}]$ is a power of 2 if and only if $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ is. However, we know that $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(n)$, so the regular n-gon is constructible if and only if $\phi(n)$ is a power of 2. If we have $n = p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k}$, then we have $\phi(n) = (p_1 - 1)(p_2 - 1)\cdots(p_k - 1)p_1^{m_1-1}p_2^{m_2-1}\cdots p_k^{m_k-1}$. For this to be a power of 2, we need all the $p_i - 1$ and all the $p_i^{m_i-1}$ to be powers of 2. If p_i is an odd prime, this happens only if p_i is a Fermat prime and $m_i = 1$.

35. *Let F be a field of characteristic zero. Show that if K is the splitting field of $x^n - a$ over F, then $G(K/F)$ is solvable.*

Let E be the nth cyclotomic extension of F. Then E is a normal extension of F, and we know that $G(E/F)$ is isomorphic to the group of integers coprime to n under multiplication modulo n, so it is abelian. We also have that $\{e\} \leqslant G(K/E) \leqslant G(K/F)$ is a subnormal series for $G(K/F)$, and the last factor group is isomorphic to $G(K/F)$, so we just need to show that $G(K/E)$ is abelian. Let β be a zero of $x^n - a$. Let ζ be a primitive nth root of unity. The zeros of $x^n - a$ are $\beta, \zeta\beta, \ldots, \zeta^{n-1}\beta$. This means that $K = E(\beta)$, so an automorphism $\sigma \in G(K/E)$ is entirely determined by $\sigma(\beta)$, and since it must preserve ζ, it must induce a cyclic permutation on $\beta, \zeta\beta, \ldots, \zeta^{n-1}\beta$, so these cyclic permutations commute, so $G(K/E)$ is abelian. Therefore, $G(K/F)$ is solvable.

36. *Show that if E is a normal extension of F and K is an extension of F by radicals, with $F \leqslant E \leqslant K$, then $G(E/F)$ is solvable.*

Let $K = F(\alpha_1, \ldots, \alpha_k)$, where $\alpha_i^{n_i} \in F(\alpha_1, \ldots, \alpha_{i-1})$, for each i. We proceed by induction to extend K to a normal extension of F by radicals.

We let $L_0 = F$, and then let L_i be the splitting field of $\mathrm{Irr}(\alpha_i, F)$ over L_{i-1}. Since we know that α_i is a zero of $x^{n_i} - \alpha_i^{n_i}$, it is also a zero of $g(x) = \Pi_{\sigma \in G(L_{i-1}/F)}(x^{n_i} - \sigma(\alpha_i^{n_i}))$, which is a polynomial in $F[x]$. We see that in L_{i-1}, $g(x)$ is a product of polynomials of the form $x^{n_i} - b$, so each L_i is a radical extension of L_{i-1}, and therefore $G(L/F)$ is solvable. Now we have that $G(E/F) \cong G(L/F)/G(L/E)$ is a factor group of a solvable group and therefore solvable.

37. Show that any transitive subgroup of S_5 which contains a transposition is the whole of S_5.

Let H be a transitive subgroup of S_5 which contains a transposition (ij). We will show that H contains all transpositions, and is therefore, the whole of S_5. We know that for any $\sigma \in H$, $\sigma(ij)\sigma^{-1} = (\sigma(i)\sigma(j))$, so since H is transitive, it contains at least one transposition (ij) for any i. Since 5 is odd, it must contain two transpositions (ij) and (ik) for some i. Now it must also contain $(ij)(ik)(ij) = (jk)$. Since H is transitive, there must be some σ sending i to an element not in $\{i, j, k\}$. On the other hand, we must have $\sigma(j) \in \{i, j, k\}$ or $\sigma(k) \in \{i, j, k\}$. This means we have a transposition (xl) where $x \in \{i, j, k\}$ and $l \notin \{i, j, k\}$. Using this and the existing transpositions, we see that any permutation on $\{i, j, k, l\}$ is possible. Finally, there is some σ sending i to the final element not in $\{i, j, k, l\}$. Conjugation by this σ gives a transposition with this element and another element. Composition with elements already obtained gives the whole of S_5.

38. Show that the quintic polynomial $f(x) = x^5 - 8x + 6$ is not solvable by radicals over $\mathbb{Q}$.

We not that f is irreducible by Eisenstein's criterion with $p = 2$. Let it have 5 zeros α, β, γ, δ and ϵ. We know that $\alpha + \beta + \gamma + \delta + \epsilon = 0$, and $\alpha\beta + \alpha\gamma + \alpha\delta + \alpha\epsilon + \beta\gamma + \beta\delta + \beta\epsilon + \gamma\delta + \gamma\epsilon + \delta\epsilon = 0$. This gives $\alpha^2 + \beta^2 + \gamma^2 + \delta^2 + \epsilon^2 = 0$, so the zeros cannot all be real. On the other hand, we have $f(-2) = -10$, $f(0) = 6$ and $f(1) = -1$, so by the intermediate value theorem, there are at least two real zeros. Non-real zeros occur in conjugate pairs, so there are an even number of them, which must be exactly two. Let K be the splitting field of f over $\mathbb{Q}$. We know that $G(K/\mathbb{Q})$ is a subgroup of S_5. It is transitive, because we have the conjugation isomorphisms. Complex conjugation is in this group and induces a transposition on the two non-real zeros of f, $G(K/\mathbb{Q})$ contains a transposition and is transitive, so it is the whole of $\mathbb{S}_5$. S_5 is not solvable, so f is not solvable by radicals over $\mathbb{Q}$.

39. Let $E = F(\alpha_1, \ldots, \alpha_n)$ be an algebraic extension of F. Show that any isomorphism σ from E to a subfield of $\overline{F}$, that leaves F fixed is uniquely determined by the values $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$.

Let σ_1 and σ_2 be two isomorphisms from E to a subfield of $\overline{F}$, that leave F fixed, such that for each i, $\sigma_1(\alpha_i) = \sigma_2(\alpha_i)$. We need to show that

$\sigma_1 = \sigma_2$. Let $S = \{x \in F(\alpha_1, \ldots, \alpha_n) | \sigma_1(x) = \sigma_2(x)\}$. We need to show that $S = F(\alpha_1, \ldots, \alpha_n)$. We know that S contains $F, \alpha_1, \ldots, \alpha_n$, so we just need to show that S is a subfield. Since σ_1 and σ_2 are homomorphisms, S must be closed under addition and multiplication. Furthermore, since $-1 \in F \subseteq S$, S is closed under additive inverse. We need to show that S is closed under multiplicative inverses. Let $\sigma_1(x) = \sigma_2(x)$. We need to show that $\sigma_1(x^{-1}) = \sigma_2(x^{-1})$. However, we know that $\sigma_1(x)\sigma_1(x^{-1}) = \sigma_1(1) = 1 = \sigma_2(1) = \sigma_2(x)\sigma_2(x^{-1}) = \sigma_1(x)\sigma_2(x^{-1})$. Therefore, multiplying by $(\sigma_1(x))^{-1}$ (which exists because σ_1 is an isomorphism, so its kernel is trivial, so $\sigma_1(x) \neq 0$) we get that $\sigma_1(x^{-1}) = \sigma_2(x^{-1})$. Therefore S is a subfield of $F(\alpha_1, \ldots, \alpha_n)$ containing F and $\{\alpha_1, \ldots, \alpha_n\}$, so it must be the whole of $F(\alpha_1, \ldots, \alpha_n)$.

New questions

40. Show that the algebraic closures of $\mathbb{Q}(\pi)$ and $\mathbb{Q}(e)$ are isomorphic.

Since π and e are both transcendental over $\mathbb{Q}$, there is an isomorphism $\sigma : \mathbb{Q}(\pi) \longrightarrow \mathbb{Q}(e)$. This extends to an isomorphism $\hat{\sigma}$ from $\overline{\mathbb{Q}(\pi)}$ to a subfield of $\overline{\mathbb{Q}(e)}$. Similarly $\hat{\sigma}^{-1}$ extends to an isomorphism from $\overline{\mathbb{Q}(e)}$ to a subfield of $\overline{\mathbb{Q}(\pi)}$. However, $\hat{\sigma}^{-1}$ is already onto $\overline{\mathbb{Q}(\pi)}$, this extension must be $\hat{\sigma}^{-1}$ itself. Therefore, $\hat{\sigma}$ must be onto $\overline{\mathbb{Q}(e)}$, so $\overline{\mathbb{Q}(\pi)}$ and $\overline{\mathbb{Q}(e)}$ are isomorphic.

41. Show that if $[E : F] = 2$, then E is a splitting field over F.

Let $\alpha \in E \setminus F$. We have that $E = F(\alpha)$, and $\deg(\alpha, F) = 2$. Let $f = \mathrm{Irr}(\alpha, F)$. Since f is a quadratic, when we divide by $(x - \alpha)$, we get a linear factor, which must have a zero in $F(\alpha)$, so f splits in $F(\alpha)$, and $F(\alpha)$ is the splitting field of F.

42. Let $E = F(\alpha)$ be a splitting field over F, and $[E : F] = 3$. Let the conjugates of α over F be β and γ. Suppose that $\sigma \in G(E/F)$ is such that $\sigma(\alpha) = \beta$. What is $\sigma(\beta)$?

Since α has two conjugates over F, E is a separable extension of F. Since $[E : F] = 3$, we have that $|G(E/F)| = 3$. The only group of order 3 is the cyclic group. This must act by cyclic permutation on the conjugates of α, so if $\sigma(\alpha) = \beta$, we must have $\sigma(\beta) = \gamma$.

43. Show that if α and β are both separable over F, then so is $\alpha + \beta$.

Since $\mathrm{Irr}(\beta, F(\alpha))$ divides $\mathrm{Irr}(\beta, F)$, we get that β is separable over $F(\alpha)$. Therefore, we have that $F(\alpha, \beta)$ is separable over F. Since $F(\alpha + \beta)$ is a subfield of $F(\alpha, \beta)$, it must also be separable over F, which means that $\alpha + \beta$ is separable over F.

44. Is every algebraically closed field perfect? Give a proof or a counterexample.

Every algebraically closed field is perfect, since the only finite extension of an algebraically closed field is the trivial extension, which is clearly separable.

45. Let $F \leqslant E \leqslant K$, where K is a normal extension of F. If $G(K/F)$ is abelian, show that $G(K/E)$ and $G(E/F)$ are both abelian.

We have that $G(K/E)$ is a subgroup of $G(K/F)$, which is abelian, so $G(K/E)$ is a subgroup of an abelian group, and therefore abelian. Now any subgroup of an abelian group is normal, so E is a normal extension of F, and we have that $G(E/F) \equiv G(K/F)/G(E/F)$, which is a factor group of an abelian group, and therefore abelian.

46. Let $f = a_0 + a_1x + \cdots + a_nx^n$ be an irreducible polynomial in $F[x]$. Let α be a zero of F. Let K be the splitting field of f over F. Recall that the norm of α over F is given by

$$N_{K/F}(\alpha) = \Pi_{\sigma \in G(K/F)}\sigma(\alpha)$$

Suppose that $[K : F] = n$. Describe $N_{K/F}(\alpha)$ in terms of the coefficients of f.

Since $[K : F] = n$, we know that $|G(K/F)| \leqslant n$. On the other hand, $G(K/F)$ acts transitively on the conjugates of α, which are the n zeros of f, so we know that for any zero α' of f, there is exactly one $\sigma \in G(K/F)$ with $\sigma(\alpha) = \alpha'$. Therefore $N_{K/F}(\alpha)$ is the product of all the conjugates of α, which is $(-1)^n a_0$.

47. Let $f(x) = x^3 + ax^2 + bx + c$ be an irreducible polynomial in $F[x]$, where F is a field of characteristic 3. Show that if f is not separable over F, then $a = b = 0$.

If f is not separable, then since all zeros have the same multiplicity, this must divide 3, so all zeros have multiplicity 3. This means that $f(x) = (x-\alpha)^3$, where α is the unique zero of f. This gives $f(x) = x^3 - 3\alpha + 3\alpha^2 - \alpha^3$, which since F has characteristic 3, is equal to $x^3 - \alpha^3$, so $a = b = 0$.

48. Let K be a finite normal extension of F. Let $\alpha \in K$. Show that $f(x) = \Pi_{\sigma \in G(K/F)}(x - \sigma(\alpha))$ is a power of $\mathrm{Irr}(\alpha, F)$.

We know that the zeros of $\mathrm{Irr}(\alpha, F)$ are the conjugates of α, and they each have multiplicity one. On the other hand, in $f(x)$, since we have conjugation isomorphisms, we know that all conjugates of α are zeros of f. Furthermore, we know that $\{\sigma \in G(K/F) | \sigma(\alpha) = \alpha'\} = \{\sigma \in G(K/F) | \tau\sigma(\alpha) = \tau(\alpha')\}$, so the number of factors for each conjugate of α is the same. Therefore, f is a power of $\mathrm{Irr}(\alpha, F)$.

49. Let m and n be coprime. Show that the mnth cyclotomic extension of $\mathbb{Q}$ is the splitting field of $\{x^m - 1, x^n - 1\}$ over $\mathbb{Q}$.

Let ζ be a primitive mnth root of unity. Then the mnth cyclotomic extension of $\mathbb{Q}$ is $\mathbb{Q}(\zeta)$. Meanwhile, ζ^m is a zero of $x^n - 1$, and ζ^n is a

zero if $x^m - 1$, so the splitting field of $\{x^m - 1, x^n - 1\}$ contains $\mathbb{Q}(\zeta^m, \zeta^n)$. However, we can find integers a and b so that $am + bn = 1$. This means $\zeta = (\zeta^m)^a(\zeta^n)^b \in \mathbb{Q}(\zeta^m, \zeta^n)$. It is obvious that $x^m - 1$ and $x^n - 1$ split in $\mathbb{Q}(\zeta)$, so we have shown both inclusions, as required.

50. *Show that if K is a finite extension of F, and F is the fixed field of $G(K/F)$, then K is a splitting field over F.*

Let $\alpha \in K$. We need to show that K contains all conjugates of α over F. Let the conjugates of α over F that are in K be $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$. Since any $\sigma \in G(K/F)$ permutes these, any symmetric function of these is left fixed by σ. Therefore, the elementary symmetric functions of $\alpha_1, \ldots, \alpha_n$ are in $K_{G(K/F)}$, so the polynomial $\Pi_{i=1}^n(x - \alpha_i)$ is in $K_{G(K/F)}[x] = F$. Therefore, this is the irreducible polynomial for α over K. Therefore, $\alpha_1, \ldots, \alpha_n$ are all the conjugates of α over F, so K is a splitting field over F.

51. *Let f be an irreducible polynomial over F. Let α be a zero of f. Show that if α lies in a radical extension E of F, then all other zeros of f also lie in radical extensions of F.*

Let R be a radical extension of F containing α, and let α' be another zeros of f. The other zeros are conjugate to α over F, so we have the conjugation isomorphism $\psi_{\alpha,\alpha'} : F(\alpha) \xrightarrow{F} (\alpha')$. This extends to an isomorphism σ from R to a subfield R' of $\overline{F}$. This R' clearly contains $F(\alpha')$, so we just need to show that it is a radical extension of F. Suppose $R = F(\beta_1, \ldots, \beta_k)$ where ${\beta_i}^{n_i} \in F(\beta_1, \ldots, \beta_{i-1})$. Now since σ is an isomorphism, we have that $\sigma(\beta_i)^{n_i} = \sigma({\beta_i}^{n_i}) \in F(\sigma(\beta_1), \ldots, \sigma(\beta_{i-1}))$, so that $R' = F(\sigma(\beta_1), \ldots, \sigma(\beta_k))$ is an extension of F by radicals.

52. *Let R be an extension of F by radicals, and let $F \leqslant E \leqslant R$ be an intermediate field. Must E be an extension of F by radicals? Give a proof or a counterexample.*

E does not need to be an extension of F by radicals. For example, if ζ is a primitive 9th root of unity, then $F(\zeta + \zeta^{-1})$ is an intermediate field, but is not an extension of $\mathbb{Q}$ by radicals.

Bonus Questions

53. *If G is a group of automorphisms of E, and is isomorphic to S_3, must E be a splitting field over E_G?*

It must (in fact this is true for any group G of automorphisms of E. Let $\alpha \in E$, we need to show that all conjugates of α over E_G are in E. However, we know that $f(x) = \Pi_{\sigma \in G}(x - \sigma(\alpha))$ is left fixed by all elements of G, so $f \in E_G[x]$, and α is a zero of f. Therefore $\mathrm{Irr}(\alpha, E_G)$ divides f,

so all conjugates of α over F are zeros of f, which are all in E. Therefore, all conjugates of α are in E, so E is a splitting field over E_G.