Demonstration of Ability to Explain Algebra Concepts to Undergraduate Students

Princeton Algebra Qualifying Exam Questions

Caitlin Beecham

1 Fields and Galois Theory

Question 1.1. *What is a separable extension? Can $\mathbb{Q}$ have a non-separable extension? How about $\mathbb{Z}/p\mathbb{Z}$? Why not? Are all extensions of characteristic 0 fields separable? Of finite fields? Prove it. Give an example of a field extension that's not separable.*

Q: What is a separable extension?
A: It is a finite field extension K/F of the form $K \cong \mathbb{F}[x]/(p(x))$ where $p(x) \in \mathbb{Q}[x]$ is separable (and of course irreducible).

Q: Can $\mathbb{Q}$ have a non-separable extension?
A: $\mathbb{Q}$ cannot. Neither can $\mathbb{Z}/p\mathbb{Z}$. The reason is that any irreducible polynomial over either of those fields in separable.

Q: Are all extensions of characteristic 0 fields separable?
A: Yes, and the key to the proof is to note that $gcd(p(x), p'(x)) \notin \mathbb{Q}^\times$. The classic argument works for $\mathbb{Q}$ and $\mathbb{Z}/p\mathbb{Z}$ but fails for $\mathbb{F}_p(t)$ for example since $\mathbb{F}_p(t)$ is not an algebraic extension of $\mathbb{F}_p$, but that is a minor point to flesh out.

Question 1.2. *Are there separable polynomials of any degree over any field?*

Yes.

For an infinite field, F, and given degree $N \in \mathbb{N}$ one may simply pick N distinct elements $\{a_i : i \in [n]\} \subseteq F$ of the field and note that $\prod_{i\in[n]}(x - a_i)$ is separable.

For a finite field the answer is also yes. Any finite field has the form $\mathbb{F}_{p^m}$ for some prime p and $m \in \mathbb{N}_{\geq 1}$. Namely, if $F = \mathbb{F}_p$ then I claim that $[\mathbb{F}_{p^N} : \mathbb{F}_p] = N$ which then implies by the primitive element theorem that there exists an element $\alpha \in \mathbb{F}_{p^N}$ whose minimal polynomial over $\mathbb{F}_p$ has degree N. Since all finite fields are perfect (meaning by definition that all irreducible polynomials over the field are separable) this minimal polynomial is separable and of the specified degree. Similarly if we are given another finite field (which is necessarily of the form $\mathbb{F}_{q^m}$ for some prime q) and want to find a separable polynomial of degree N. We consider the field $\mathbb{F}_{q^{mN}}$ and since I claim that $[\mathbb{F}_{q^{mN}} : \mathbb{F}_{q^m}] = N$ which implies by the primitive element theorem that $\mathbb{F}_{q^{mN}} = \mathbb{F}_{q^m}(\beta)$ for some $\beta \in \mathbb{F}_{q^{mN}}$ with minimal polynomial

over $\mathbb{F}_{q^m}$ of degree N. Then, one again since all finite fields are perfect and any minimal polynomial is irreducible, this polynomial is separable and of the desired degree.

Question 1.3. *What is a perfect field and why is this important? Give an example of a non-perfect field.*

It is a field over which every irreducible polynomial is separable. This is important because it implies for instance that, for a perfect field, the splitting field of any irreducible polynomial over the field is Galois. If the field were not perfect, one would also have to ensure that the minimal polynomial of a primitive element generating the extension were separable, but in this case one does not.

Question 1.4. *What is Galois theory? State the main theorem. What is the splitting field of $x^5 - 2$ over $\mathbb{Q}$? What are the intermediate extensions? Which extensions are normal, which are not, and why? What are the Galois groups (over $\mathbb{Q}$) of all intermediate extensions?*

It is the study of field extensions, how to construct them, and the automorphisms of said fields fixing certain subfields.

Now, we determine the splitting field of $h(x) = x^5 - 2$ over $\mathbb{Q}$. Note that $x^5 - 2 = \prod_{k\in[5]}(2)^{1/5}\zeta_5^k$ and thus the splitting field is certainly not

$$\mathbb{Q}/(h(x))$$

since $\mathbb{Q}/(h(x)) \cong \mathbb{Q}(2^{1/5}) \subseteq \mathbb{R}$ meaning that the other roots are not contained in $\mathbb{Q}/(h(x))$ since they are not real for instance. However, if one then lets $g(x) \in \mathbb{Q}/(h(x))$ be defined as the minimal polynomial $m_{\zeta_5,\mathbb{Q}(2^{1/5})}$ of ζ_5 over $\mathbb{Q}(2^{1/5}) \cong \mathbb{Q}/(h(x))$, then we ask whether $\mathbb{Q}(2^{1/5})/(m_{\zeta_5,\mathbb{Q}(2^{1/5})})$ is the splitting field. Indeed it is. Note that $2^{1/5}\zeta_5^k \in \mathbb{Q}(2^{1/5})(\zeta_5)$ since $\mathbb{Q}(2^{1/5})(\zeta_5)$ is a field and thus closed under multiplication.

For finite degree extensions, there is a correspondence between subfields of a Galois field extension and subgroups of the associated Galois group. Namely,

$$K = \mathbb{F}(\alpha)$$

is the field extension obtained by adjoining α to $\mathbb{F}$ and then taking the closure (meaning smallest field containing $\mathbb{F}$ and α). Equivalently, we have that $K \cong \mathbb{F}[x]/(m_\alpha(x))$ where $m_\alpha(x)$ is the minimal polynomial of α over $\mathbb{F}$. If the "Galois group" of K is the group of automorphisms of K fixing $\mathbb{F}$ pointwise, denoted $Gal(K/\mathbb{F})$, then the Fundamental Theorem of Galois theory states that for each subgroup $H \subseteq Gal(K/\mathbb{F})$ there exists a field E with $\mathbb{F} \subseteq E \subseteq K$ such that

$$Gal(K/E) \cong H.$$

Intermediate fields are simply fields containing one field and contained in another.

Normal extensions K of F are those which are the splitting field of an irreducible polynomial over F.

Question 1.5. *What is a Galois extension?*

It is an extension that is both normal and separable. (A separable field extension is a finite extension $K = \mathbb{F}(\alpha)$ whose minimal polynomial $m_\alpha(x)$ is separable). (Equivalently, it is a finite extension $K/\mathbb{F}$ such that $|Aut(K/\mathbb{F})| = [K : \mathbb{F}]$). (Equivalently, Galois extensions are those that are splitting fields of irreducible, separable polynomials).

Question 1.6. *Take a quadratic extension of a field of characteristic* 0*. Is it Galois? Take a degree* 2 *extension on top of that. Does it have to be Galois over the base field? What statement in group theory can you think of that reflects this?*

Yes. Since it is quadratic we have that $K = \mathbb{F}/(f(x))$ where $f(x) = (x - a_1)(x - a_2)$ is irreducible over $\mathbb{F}$ and where $a_1, a_2 \in \overline{\mathbb{F}}$. To show that the extension is Galois, it suffices to show that the above polynomial splits in K (normality) and that the above polynomial is separable (separability). So, first note that $f(x) = x^2 - (a_1 + a_2)x + a_1a_2$. Also, note that $K = \mathbb{F}/(f(x)) \cong \mathbb{F}(a_1) \cong \mathbb{F}(a_2)$. To show normality we must show that $a_2 \in \mathbb{F}(a_1)$. Well, $a_1a_2 \in \mathbb{F}$ since $f(x) \in \mathbb{F}[x]$ by assumption and then $a_2 = \frac{a_1a_2}{a_1} \in \mathbb{F}(a_1)$ since $\mathbb{F}(a_1)$ is closed under division by units where we are using the fact that $a_1 \neq 0$ since $f(x)$ was irreducible over $\mathbb{F}$ (meaning 0 was not a root). Now, to show separability we show that $a_1 \neq a_2$. Otherwise, if $a_1 = a_2$ that implies that $f(x) = (x - a_1)^2 = x^2 - 2a_1 + a_1^2$ but $a_1 \notin \mathbb{F}$ implies that $-2a_1 \notin \mathbb{F}$ since if so, the fact that $char(\mathbb{F}) \neq 2$, implies that -2 is a unit and thus $a_1 \in \mathbb{F}$, providing a contradiction.

Question 1.7. *Is abelian Galois extension transitive? That is, if K has abelian Galois group over E, E has abelian Galois group over F, and K is a Galois extension of F, is it necessarily true that* $\mathrm{Gal}(K/F)$ *is also abelian? Give a counterexample involving number fields as well as one involving function fields.*

No, not necessarily. Take $K = \mathbb{Q}(2^{1/3}, \zeta_3)$ defined as $K = E[x]/(x^3 - 2)$ and $E = \mathbb{Q}(x)/(x^2 + x + 1)$. Note that $k/\mathbb{Q}$ is a Galois field extension since $|Aut(K/\mathbb{Q})| = [K : \mathbb{Q}]$. (Note that $[K : \mathbb{Q}] = 6$ since $[K : \mathbb{Q}] = [K : E][E : \mathbb{Q}] = 3 * 2$). (Also, the reason I know that $|Aut(K/\mathbb{Q})| = 6$ is because $Aut(K/\mathbb{Q}) = \langle \phi, \psi \rangle$ where $\phi(2^{1/3}) = 2^{1/3}\zeta_3$, $\phi(\zeta_3) = \zeta_3$ and $\psi(\zeta_3) = \zeta_3^2$, $\psi(2^{1/3}) = 2^{1/3}$ which indeed gives $\langle \phi, \psi \rangle \cong S_3$. So, clearly $Gal(K/\mathbb{Q})$ is not abelian. However, $E/\mathbb{Q}$ is Galois since it is a degree 2 extension over a field of characteristic 0 meaning we can use 3.12, which implies its Galois group had order 2 (degree of the extension = degree of relevant minimal polynomial) and is thus the abelian group $\mathbb{Z}_2$. Also, K/E is Galois since $|Gal(K/E)| = deg(x^3 - 2)$. In particular, $Gal(K/E) = \langle \sigma \rangle \cong \mathbb{Z}_3$ where $\sigma(2^{1/3}) = 2^{1/3}\zeta_3$ and is thus abelian. However $Gal(K/\mathbb{Q}) \cong S_3$ is not abelian. So, we have a non-abelian Galois extension constructed via two successive abelian Galois extensions.

Now, to give an example using function fields we define $F = \mathbb{Q}(t)$, $E = F[x]/(x^2 + x + 1)$ and $K = E[x]/(x^3 - 2)$. The argument is nearly the same. In particular, I claim that K/F is Galois with $Gal(K/F) = S_3$ once again. Since t is transcendental over $\mathbb{Q}$ that means that $f(x)$ with coefficients in $\mathbb{Q}$ is irreducible over $\mathbb{Q}$ if and only if it is irreducible over $\mathbb{Q}(t)$ (still only allowing coefficients in $\mathbb{Q}$). Thus, $x^2 + x + 1$ is irreducible over $F = \mathbb{Q}(t)$ and by the same argument as 3.12 E is the splitting field of the separable polynomial $x^2 + x + 1$. Thus, $E/\mathbb{Q}(t)$ is Galois with order two Galois group $\mathbb{Z}_2$ (the only group of order 2). Now, we see

again that $Gal(k/\mathbb{Q}) = \langle \sigma, \tau \rangle \cong S_3$ where $\sigma(\alpha) = \alpha\beta, \sigma(\beta) = \beta$, $\tau(\alpha) = \alpha$ and $\tau(\beta) = \beta^2$ where α is a root of $x^3 - 2$ and β is a root of $x^2 + x + 1$. Finally, since any automorphism $\sigma \in Aut(K/\mathbb{Q}(t)) \cong Aut(K(\alpha, \beta)/\mathbb{Q}(t))$ is completely determined by the values $\sigma(\alpha), \sigma(\beta)$, that means that verifying that $\langle \sigma, \tau \rangle \cong S_3$ concludes the proof that $Gal(K/\mathbb{Q}(t)) \cong S_3$. Then, we have that $|Gal(K/F)| = 6 = deg(K/F)$ meaning K/F is Galois which then implies that K/E is Galois (by a well-known theorem about towers of extensions). So, indeed we have obtained another counterexample.

Question 1.8. *Tell me a condition on the Galois group which is implied by irreducibility of the polynomial. What happens when the polynomial has a root in the base field?*

It acts transitively on the roots of the polynomial. For instance, $\mathbb{Q}(\sqrt{2}, i)$ can be constructed either as $(\mathbb{Q}[x]/(x^2 - 2))/(x^2 + 1)$ or as $\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(m_\alpha(x))$ according to the primitive element theorem. Now, by observing the first construction it is quite clear why, intuitively $Gal(\mathbb{Q}(\sqrt{2}, i)) = \mathbb{Z}_2 \times \mathbb{Z}_2$. However, the above construction was not done by quotient-ing in one step by the ideal generated by an irreducible polynomial (which is necessary to get a field, since we must quotient a ring by a maximal ideal to obtain a field).

So, we see that the Galois group does not act transitively on the roots of $(x^2 - 2)(x^2 + 1)$. However, the same group (meaning the exact same set of automorphisms) DOES act transitively on the roots of $m_\alpha(x)$. (I suppose one could think of this condition as saying that the roots are indistiguishable as part of the structure of the extension field, which is why we obtain isomorphic field extensions no matter which root of the specified minimal polynomial we adjoin to the base field).

If the polynomial has a root in the base field, the Galois group will not act transitively on the roots. Namely, consider $\mathbb{Q}(\zeta_3) \cong \mathbb{Q}[x]/(x^2 + x + 1)$ and note that $x^3 - 1$ certainly does split in $\mathbb{Q}(\zeta_3)$. However, for one of the roots of $x^3 - 1$, namely 1, we see that no automorphism $\sigma \in Aut(\mathbb{Q}(\zeta_3)/\mathbb{Q})$ takes 1 to another root of the equation $x^3 - 1$. (This is one example of what I meant about roots of an irreducible polynomial being "indistinguishable" as far as the structure of the field is concerned. The element 1 is definitely distinguisable from any other element, just as an element $q \in \mathbb{Q}$ is distinguishable (solely using field structure, i.e. equations the element satisfies over the field $\mathbb{Q}$) from elements of $\mathbb{Q}(i) \setminus \mathbb{Q}$).

Question 1.9. *Is $\mathbb{Q}(2^{1/3})$ normal? What is its splitting field? What is its Galois group? Draw the lattice of subfields.*

No. If it were normal, every polynomial with a root in the field would split. However, $x^3 - 2$ does not split. Its splitting field is $K := \mathbb{Q}(2^{1/3}, \zeta_3)$. Its Galois group is $Gal(K/\mathbb{Q}) = \langle \phi, \psi \rangle$ where $\phi(2^{1/3}) = 2^{1/3}\zeta_3$, $\phi(\zeta_3) = \zeta_3$ and $\psi(\zeta_3) = \zeta_3^2$, $\psi(2^{1/3}) = 2^{1/3}$ which indeed gives $\langle \phi, \psi \rangle \cong S_3$. Note that any autmorphism in $Gal(K/\mathbb{Q})$ is generated by ϕ, ψ since any automorphism must send roots of a given polynomial (such as $x^2 + x + 1$ or $x^3 - 2$) to other roots of that polynomial.

The subfields correspond to subgroups of S_3. Namely, they are the fixed fields of the following subgroups: $\{id\}$, $\langle \phi \rangle$, $\langle \psi \rangle$, $\langle \phi^{-1} \circ \psi \circ \phi \rangle$, $\langle \phi \circ \psi \circ \phi^{-1} \rangle$, $\langle \psi^{-1} \circ \phi \circ \psi \rangle$, and $\langle \phi, \psi \rangle$.

Question 1.10. *What's the Galois group of x^2+1 over $\mathbb{Q}$? What's the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(i)$?*

The Galois group is $\mathbb{Z}_2$. The integral closure in $\mathbb{Q}(i)$ is $\mathbb{Z}[i]$. So, we must show that any algebraic element has this form and that any element of that form satisfies an irreducible monic polynomial with integer coefficients.

Question 1.11. *What's the Galois group of x^2+9?*

Note that $x^2+9=(x+3i)(x-3i)$ and thus $\mathbb{Q}[x]/(x^2+9)$ is a normal and separable extension (meaning Galois). Its Galois group is $\mathbb{Z}_2$ since $\mathbb{Z}_2$ is the only group of order 2 and the size of a Galois group is the degree of the extension (which is 2).

Question 1.12. *What is the Galois group of x^2-2? Why is x^2-2 irreducible?*

It is $\mathbb{Z}_2$. See above. It is irreducible because otherwise x^2-2 would split in $\mathbb{Q}$, but it does not since $\pm\sqrt{2}\notin\mathbb{Q}$.

Question 1.13. *What is the Galois group of $\mathbb{Q}(\sqrt{2},\sqrt{3})$ over $\mathbb{Q}$?*

It is $\mathbb{Z}_2\times\mathbb{Z}_2$.

Question 1.14. *What is the Galois group of $\mathbb{Q}(\sqrt{n_1},\sqrt{n_2},\ldots,\sqrt{n_m})$ over $\mathbb{Q}(\sqrt{n_1}+\ldots+\sqrt{n_m})$?*

I am assuming that n_i are not squares. I am also assuming that if $n_i \mid n_j$ for some $i\neq j$ then n_j/n_i is not a square. (Because then $n_j\in\mathbb{Q}(n_i)$ since $n_j=n_ib^2$ meaning that $\sqrt{n_j}=\sqrt{n_i}b$). I will actually just assume directly that $\sqrt{n_j}\notin\mathbb{Q}(\sqrt{n_1},\ldots,\sqrt{n_{j-1}})$.

First, let me handle two simpler cases so that I can see the proof pattern. Namely consider $\mathbb{Q}(\sqrt{2},\sqrt{3})$ over $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ and $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$ over $\mathbb{Q}(\sqrt{2}+\sqrt{3}+\sqrt{5})$.

So, what is the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}(\sqrt{2}+\sqrt{3})$? Well, over $\mathbb{Q}$ it is x^2-2 and certainly since $\sqrt{2}\notin 2$ we know that the degree of the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ is at least 2 and since $x^2-2\in\mathbb{Q}(\sqrt{2}+\sqrt{3})$, it is the minimal polynomial. Then, I claim that $\sqrt{3}\in\mathbb{Q}(\sqrt{2}+\sqrt{3})(\sqrt{2})$ since $\sqrt{3}=\sqrt{2}+\sqrt{3}-\sqrt{2}$. Thus, $\mathbb{Q}(\sqrt{2},\sqrt{3})$ is generated as $\mathbb{Q}(\sqrt{2}+\sqrt{3})/(x^2-2)$. Thus its Galois group is $\mathbb{Z}_2$. Now, we consider the more complicated case of $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$ over $\mathbb{Q}(\sqrt{2}+\sqrt{3}+\sqrt{5})$. Namely, what is the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}(\sqrt{2}+\sqrt{3}+\sqrt{5})$. It is clearly of degree 2 since $\sqrt{2}$ is not in that field. So by the above argument it is x^2-2. Then, since $\sqrt{3}\notin\mathbb{Q}(\sqrt{2}+\sqrt{3}+\sqrt{5})(\sqrt{2})$ we know that its minimal polynomial has degree at least two and since x^2-3 has coefficients in $\mathbb{Q}(\sqrt{2}+\sqrt{3}+\sqrt{5})(\sqrt{2})$ that is its minimal polynomial meaning that $\mathbb{Q}(\sqrt{2}+\sqrt{3}+\sqrt{5})(\sqrt{2},\sqrt{3})=(\mathbb{Q}(\sqrt{2}+\sqrt{3}+\sqrt{5})/(x^2-2))/(x^2-3)$. Now, note that $\sqrt{5}\in\mathbb{Q}(\sqrt{2}+\sqrt{3}+\sqrt{5})(\sqrt{2},\sqrt{3})$ meaning that $Gal(\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})/\mathbb{Q}(\sqrt{2}+\sqrt{3}+\sqrt{5}))=\mathbb{Z}_2\times\mathbb{Z}_2$.

So, I then assume the pattern given my assumptions is that $Gal(\mathbb{Q}(\sqrt{n_1},\sqrt{n_2},\ldots,\sqrt{n_m})/\mathbb{Q}(\sqrt{n_1}+\ldots+\sqrt{n_m}))=(\mathbb{Z}_2)^{m-1}$.

Question 1.15. *What are the Galois groups of irreducible cubics?*

They are S_3. How do I show that? Well first show that for an irreducible cubic $p(x)$ we have that either $p(x)$ splits in $\mathbb{Q}[x]/(p(x)) \cong \mathbb{Q}(a_1)$ (where a_1 is any root of $p(x)$) or it doesn't. If it does, its Galois group has order 3, which means the group is $\mathbb{Z}_3$. If it doesn't then the splitting field is $(\mathbb{Q}[x]/(p(x)))/(q(x)) =: K$ where $deg(q(x)) \leq 3$ since the minimal polynomial of a root a_3 (there was at least one not in $\mathbb{Q}(a_1)$ which is WLOG a_3) of $q(x)$ over $(\mathbb{Q}[x]/(p(x)))$ divides any polynomial over $(\mathbb{Q}[x]/(p(x)))$ which has it as a root. So, in particular, it divides $p(x)$ (since $\mathbb{Q} \subseteq (\mathbb{Q}[x]/(p(x)))$) meaning that if $p(x) = (x-a_1)(x-a_2)(x-a_3)$ we have that $q(x) \mid p(x)$ and thus $q(x) = (x-a_2)(x-a_3)$ (since a_1, a_2, a_3 are the roots of p in "the" algebraic closure and since $x - a_3$ cannot be the minimal polynomial since $a_3 \notin \mathbb{Q}(a_1)$ and since the minimal polynomial is irreducible over $\mathbb{Q}(a_1)$ meaning it cannot have $(x-a_1)$ as a factor). Then, since any quadratic polynomial splits in its quadratic extension we have that $Gal(K/\mathbb{Q}(a_1)) = \mathbb{Z}_2$ and $Gal(\mathbb{Q}(a_1)/\mathbb{Q}) = \{e\}$ (since $a_2, a_3 \notin \mathbb{Q}(a_1)$ since otherwise if one was then the minimal polynomial $(x-a_2)(x-a_3)$ of a_3 would have a root in $\mathbb{Q}(a_1)$ and thus be reducible, a contradiction). Then, that means the Galois group has order 6 and is thus either $\mathbb{Z}_2 \times \mathbb{Z}_3$ or S_3.

I first show that the polynomial $p(x)$ cannot split in $\mathbb{Q}[x]/(p(x))$. In particular, any cubic has a real root which is a_1 without loss of generality and $\mathbb{Q}[x]/(p(x)) \cong \mathbb{Q}(a_1) \subseteq \mathbb{R}$. So, if the polynomial splits completely, then all the roots must be real. In such a case we have that

$$p(x) = (x-a_1)(x-a_2)(x-a_3)$$

where $a_1, a_2, a_3 \notin \mathbb{Q}$ but

$$\frac{p(x)}{(x-a_3)} \in \mathbb{R}[x]$$

is a quadratic and thus its roots can be found using the quadratic formula and are either repeated roots in $\mathbb{Q}(a_1)$ or are roots of the form $\frac{-b \pm \sqrt{b^2-4c}}{2} \in \mathbb{Q}(a_1)$ where $b, c \in \mathbb{Q}(a_1)$. However, they are not repeated since $\mathbb{Q}$ perfect and p irreducible implies that p is separable. So, they are of the form $\frac{-b \pm \sqrt{b^2-4c}}{2}$ with $b^2 - 4c > 0$ (since they are not complex by our assumption that the polynomial splits in $\mathbb{Q}(a_1) \subseteq \mathbb{R}$). Also, by our assumption here $a_2 a_3 = c$ and $a_2 + a_3 = b$ which implies that $(a_2+a_3)^2 > 4a_2a_3$ or that $a_2^2 + a_3^2 - 2a_2a_3 > 0$.

So, we have that

$$a_2 = \frac{-b + \sqrt{b^2-4c}}{2} = \frac{-(a_2+a_3) + \sqrt{(a_2^2+a_3^2-2a_2a_3)}}{2}$$

and

$$a_3 = \frac{-b - \sqrt{b^2-4c}}{2} = \frac{-(a_2+a_3) - \sqrt{(a_2^2+a_3^2-2a_2a_3)}}{2}$$

and thus

$$a_2 + a_3 = -(a_2+a_3)$$

meaning that

$$a_2 + a_3 = 0$$

or

$$a_3 = -a_2.$$

However, now we get a contradiction since on one hand we have that $p(x) = (x - a_1)(x - a_2)(x - a_3)$ is the minimal polynomial of $\mathbb{Q}[a_2]$ but on the other hand it is not.

Namely, on one hand the fact that $p(x)$ is irreducible, $\mathbb{Q}$ is perfect (and thus all minimal polynomials are the unique irreducible polynomial with the adjoined number as a root) and has a_2 as a root implies that $p(x)$ is the minimal polynomial of $\mathbb{Q}[a_2]$ over $\mathbb{Q}$.

However, on the other hand, the roots have the form $a_2 = \frac{1}{2}\sqrt{B}$ and $a_3 = \frac{-1}{2}\sqrt{B}$ where $B = b^2 - 4c$ is a rational number. As such $p(x) = (x - a_1)(x^2 - \frac{B^2}{4})$ and since $\frac{B^2}{4}$ is rational we have that $x^2 - \frac{B^2}{4} \in \mathbb{Q}[x]$ meaning that $x^2 - \frac{B^2}{4}$ is the minimal polynomial of a_2 if $x^2 - \frac{B^2}{4}$ is irreducible or $x - a_2$ is otherwise. In any case, we get a contradiction.
Now, how can we determine the Galois group? The Galois group must define a valid group action on the roots. In particular for each a_i one must have that $Stab_G(a_i)$ is a subgroup of G. Also, by the orbit stabilizer theorem we know that since 3 is the size of our single orbit since G acts transitively on the roots that $3 = |G|/|Stab_G(a_i)| = 6/|Stab_G(a_i)|$ for all $i \in [3]$ meaning that $|Stab_G(a_i)| = 2$ for all $i \in [3]$. Also, I claim that $Stab_G(a_i) \neq Stab_G(a_j)$ for some $i \neq j \in [3]$ because otherwise the action wouldn't be transitive. Namely, if we had that $Stab_G(a_1) = Stab_G(a_2) = Stab_G(a_3)$ then for instance if G were $\mathbb{Z}_2 \times \mathbb{Z}_3$ that would mean that $(0,1)a_i \neq a_i$ for all $i \in [3]$ and that $(1,0)a_i = a_i$ for all $i \in [3]$. However, since any $\sigma \in G$ is completely determined by $\sigma(a_1), \sigma(a_2), \sigma(a_3)$ we have a contradiction since ostensibly $(0,1) \neq (1,1) \in G$ yet $(0,1)(a_i) = (1,1)(a_i)$ for all $i \in [3]$ a contradiction to $(0,1) \neq (1,1) \in G$. Thus, we have proved that $G = S_3$.

Question 1.16. *If an irreducible cubic polynomial has Galois group not contained in A_3, does it necessarily have to be all of S_3?*

Yes. The splitting field of any cubic polynomial (over an arbitrary field now) is either of degree 3 or degree 6 (I only used the real field condition from the above question to rule of degree 3). So, it is either $\mathbb{Z}_3$ or S_3. (The above argument still applies to show it is not $\mathbb{Z}_2 \times \mathbb{Z}_3$). Note that $|A_3| = |S_3|/2 = 3$ meaning that $A_3 \cong \mathbb{Z}_3$ and thus, if it is not contained in A_3 that means it is not trivial and it is not of order 3 and is thus of order 2 or 6. Its Galois group does not have order 2 since that would imply it was a degree 2 extension but it is certainly degree 3 or degree 6. Thus, it is of order 6 which I showed above means it is S_3.

Question 1.17. *Compute the Galois group of $x^3 - 2$ over the rationals.*

It is S_3 by my above argument in 3.25 (I am using the fact that $\mathbb{Q}[x] \subseteq \mathbb{R}[x]$ to be able to apply the quadratic formula and fact that complex roots come in conjugate pairs (which showed it was of order 6) and also the argument at the end (to show it wasn't $\mathbb{Z}_2 \times \mathbb{Z}_3$)).

Question 1.18. *How would you find the Galois group of $x^3 + 2x + 1$? Adjoin a root to $\mathbb{Q}$. Can you say something about the roots of $x^3 + 3x + 1$ in this extension?*

Either it is reducible or it is not. If it is reducible, then it has a root in $\mathbb{Q}$ and thus $\mathbb{Q}[x]/(x^3+2x+1) \cong \mathbb{Q}$ meaning the Galois group of x^3+2x+1 is the trivial group.

Otherwise, question 1.15 says the Galois group is S_3.

So, we must determine which is true. If it is reducible, then

$$x^3+2x+1 = (x-a_1)(x-a_2)(x-a_3)$$

where $a_1 \in \mathbb{Q}$, $a_2 = \frac{A+\sqrt{B}}{2}$, and $a_3 = \frac{A-\sqrt{B}}{2}$ for some rational A, B. Thus,

$$x^3+2x+1 = (x-a_1)(x^2-Ax+\frac{A^2-B}{4}) = (x^3+(-a_1-A)x^2+(\frac{A^2-B}{4}+a_1A)x+\frac{(-a_1)(A^2-B)}{4})$$

meaning that

$$\begin{aligned} A &= -a_1 \\ 2 = \frac{A^2-B}{4} - A^2 &= \frac{-B}{4} - \frac{3A^2}{4}1 \qquad\qquad = \frac{A(A^2-B)}{4} \end{aligned}$$

or better put

$$\begin{aligned} B &= -8-3A^2 \\ 4 &= A(A^2-B) \end{aligned}$$

and thus

$$1 = A^3+2A.$$

Also,

$$-B-3A^2 = 2A^3-2AB$$

or

$$0 = 2A^3+3A^2-2AB+B = 2A^3+3A^2+B(-2A+1) = 2A^3+3A^2+(-8-3A^2)(-2A+1) = 8A^3-8$$

so that

$$0 = 8(A^3-1)$$

meaning $A^3 = 1$ and since $A \in \mathbb{Q}$ we see $A = 1$ and thus $B = -11$. However, then $a_2 = \frac{1+\sqrt{11}}{2}$ and $a_3 = \frac{1-\sqrt{11}}{2}$, which provides a contradiction since then $1 = -a_1a_2a_3 = a_2a_3 = \frac{-10}{4}$.

Thus, $p(x)$ is irreducible and its Galois group is S_3 by 1.15.

Question 1.19. *Compute the Galois group of* x^3+6x+3.

This is irreducible over $\mathbb{Q}$ by Eisenstein. So by the above arguments it is S_3.

Question 1.20. *Find the Galois group of* x^4-2 *over* $\mathbb{Q}$.

Note that

$$x^4 - 2 = (x-2)(x^3 + bx^2 + cx + 1)$$

with $-2b + c = 0$ and $-2c + 1 = 0$ meaning that $c = 0.5$ and $b = 0.25$. So,

$$x^4 - 2 = (x-2)(x^3 + \frac{1}{4}x^2 + \frac{1}{2}x + 1).$$

Now to see whether this factors further we ask whether ± 1 is a root of the rightmost term. No, it is not, which means that this is the factorization into irreducible polynomials. Thus, the Galois group of $x^2 - 4$ is the Galois group of $x^3 + \frac{1}{4}x^2 + \frac{1}{2}x + 1$. By our above arguments that is S_3.

Question 1.21. *What's the Galois group of $x^4 - 3$?*

Note that

$$x^4 - 3 = (x-3)(x^3 + bx^2 + cx + 1)$$

where $-3b + c = 0$ and $-3c + 1 = 0$ meaning that $c = \frac{1}{3}$ and $b = \frac{1}{9}$. Thus,

$$x^4 - 3 = (x-3)(x^3 + \frac{1}{9}x^2 + \frac{1}{3}x + 1)$$

and by the rational roots theorem, the above is factored into a product of irreducible polynomials. So, the Galois group of $x^4 - 3$ is the Galois group of $(x^3 + \frac{1}{9}x^2 + \frac{1}{3}x + 1)$ which is an irreducible cubic over $\mathbb{Q}$ and is thus S_3.

Question 1.22. *What is the Galois group of $x^4 - 2x^2 + 9$?*

We first ask whether the above polynomial is irreducible. We cannot use Eisenstein's criterion, but we can first ask whether it has a rational root, which would have to be $\pm 1, \pm 3, \pm 9$. Clearly, ± 9 is not a root. Neither is ± 3. Finally we see that ± 1 are not either. So, it is either irreducible or the product of two irreducible polynomials quadratics.

If it is the product of two irreducible quadratics, then by the quadratic formula and the fact that irreducible implies separable for $\mathbb{Q}$ we know that all roots are complex.

If it is the product of two such irreducible polynomials we must have that each of their discriminants are non-zero.

Question 1.23. *Compute the Galois group of $p(x) = x^7 - 3$.*

It is some kind of semi-direct product of $\mathbb{Z}_7$ and $\mathbb{Z}_7^\times$ generated by f, g where $f(\zeta_7) = \zeta_7$ and $f(2^{1/7}) = 2^{1/7}\zeta_7$ and $\{g_k(\zeta_7) : (k, 7) = 1\}$ with $g_k(\zeta_7) = \zeta_7 k$ and $g_k(2^{1/7}) = 2^{1/7}$.

2 Normal Forms

Question 2.1. *Give the 4×4 Jordan forms with minimal polynomial $(x-1)(x-2)^2$.*

There are two, namely $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix}$ or $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix}$, due to the fact that the roots of the minimal polynomial are the eigenvalues of the matrix and the exponent associated with each root λ is the maximum size of any Jordan Blocks associated with the eigenvalue λ. We know definitively that there must be a Jordan Block of size 2 for the eigenvalue 2 and that the largest Jordan Block for the eigenvalue 1 has size 1. That leaves us with one of the two options above.

Question 2.2. *What is a nilpotent matrix?*

It is a square matrix A such that $A^n = 0$ for some power $n \in \mathbb{N}_{\geq 1}$.

Question 2.3. *When do the powers of a matrix tend to zero?*

They tend to zero when all eigenvalues have modulus (or absolute value) strictly less than 1. In such a case the power A^n tends to zero as $n \to 0$ in the sense that the modulus of the individual entries of A^n tend to zero as $n \to 0$.

Question 2.4. *Is a square matrix always similar to its transpose?*

No, that is a rare and complete coincidence when it does happen.

Question 2.5. *What are the conjugacy classes of* $\mathrm{SL}_2(\mathbb{R})$*?*

First note that the pair of eigenvalues of a matrix $A \in \mathrm{SL}_2(\mathbb{R})$ is one of $(\lambda_1, \lambda_2) \in \{(1,1), (-1,1), (i,-i)\}$ due to the fact that the product of a pair of eigenvalues is 1 and since the eigenvalues in each pair are complex conjugates of each other. Those pairs of eigenvalues constitute representatives of at least 3 conjugacy classes of $\mathrm{SL}_2(\mathbb{R})$. Now, matrices with the same eigenvalues can, a priori, belong to different conjugacy classes, but if the eigenvalues of A are distinct, then the matrix is diagonalizable and thus there is only one matrix up to conjugation, *by matrices in* $\mathbb{C}$, with eigenvalues $\lambda_1 \neq \lambda_2$ We will need to take some care to examine conjugacy classes for which the associated change-of-basis matrices must have real entries and have determinant 1, but for now, we note that the set of matrices with eigenvalue pairs $(-1,1)$ (resp. $(i,-i)$) belong to a single conjugacy class (where the change-of-basis matrices are allowed to be complex with any non-zero determinant) and since the eigenvalue pair is the same for all matrices in a conjugacy class, the set of matrices with eigenvalue pair $(-1,1)$ (resp. $(i,-i)$) constitute a conjugacy class (where the change-of-basis matrices are allowed to be complex) of $\mathrm{SL}_2(\mathbb{R})$. Now, we deal with the set of matrices with eigenvalue pair $(1,1)$. Is it possible to have matrices A, B each with eigenvalue pair $(1,1)$ who are not conjugate? Indeed it is, the matrices $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ each have eigenvalue pair $(1,1)$ but are not conjugate (even allowing the change-of-basis matrices to have complex entries, so are certainly not conjugate when only allowing the change-of-basis matrices to have real entries) since the conjugacy class of the identity matrix, $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, contains only the identity matrix (since $PIP^{-1} = PP^{-1} = I$ for any invertible matrix P). Now, since the matrix $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ is in Jordan Normal Form and the only possible Jordan Forms for matrices with the eigenvalue pair $(1,1)$ are $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. When working over an algebraically closed field, meaning allowing change-of-basis matrices to have complex entries, every matrix is similar to unique Jordan Normal Form and, as a result, two matrices are similar (over $\mathbb{C}$) if and only if they

have the same Jordan Normal Form. However $\mathbb{R}$ is not algebraically closed so we need to be a bit more careful for two reasons: one is that a matrix need not even be similar over $\mathbb{R}$ to its Jordan Normal Form; the second is really the same reason in disguise that implies that two matrices with the same Jordan Normal Form need not be similar over $\mathbb{C}$. So, now that we've discussed all the intricacies of these concepts, it is time to iron out where they need tweaking when working over $\mathbb{R}$.

Namely, need two matrices that each have the eigenvalue pair $(1, -1)$ be similar over $\mathbb{R}$? The answer is yes, since a distinct pair of eigenvectors u_1, u_2 scaled to have norms such that the change-of-basis matrix $P = \begin{pmatrix} u_1^1 & u_2^1 \\ u_1^2 & u_2^2 \end{pmatrix}$ has determinant 1. Namely, for any chosen eigenvectors u_1, u_2 for eigenvalues $1, -1$ respectively, one forms the change-of-basis matrix $P = \begin{pmatrix} u_1^1 & u_2^1 \\ u_1^2 & u_2^2 \end{pmatrix}$ from e_1, e_2 to u_1, u_2 and if $\det(P) \neq 1$ it is certainly non-zero since a pair eigenvectors for distinct eigenvalues form a linearly independent set. As such say $det(P) = a$, then we redefine (using computer science reassignment notation) $u_1 := \frac{1}{a} u_1$ which also updates the matrix $P := \begin{pmatrix} u_1^1 & u_2^1 \\ u_1^2 & u_2^2 \end{pmatrix}$ so that $\det(P) = 1$. So, we now have that $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) = P^{-1} M P$ for a matrix $P \in \mathrm{SL}_2(\mathbb{R})$. Since any two matrices $M, \hat{M} \in \mathrm{SL}_2(\mathbb{R})$ with eigenvalue pair $(1, -1)$ are each similar to $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ and similarity is a transitive property, we have that M and $\hat{M}$ are similar over $\mathbb{R}$.

We also show that any two matrices $M, \hat{M}$ that each have the eigenvalue pair $(i, -i)$ be similar over $\mathbb{R}$. Namely, say that we have the eigenvectors $w_1 = (w_1^1, w_1^2)^T$ and $w_2 = (w_2^1, w_2^2)^T$ of M associated with the eigenvalues $i, -i$ respectively chosen as above so that the change-of-basis matrix, $P = \begin{pmatrix} w_1^1 & w_2^1 \\ w_1^2 & w_2^2 \end{pmatrix}$ from e_1, e_2 to w_1, w_2. So, M is similar to $\left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right) = \begin{pmatrix} w_1^1 & w_2^1 \\ w_1^2 & w_2^2 \end{pmatrix}^{-1} M \begin{pmatrix} w_1^1 & w_2^1 \\ w_1^2 & w_2^2 \end{pmatrix}$ over $\mathrm{SL}_2(\mathbb{R})$. Now, one might take issue with the fact that $\left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right)$ has non-real entries, but the above observation is only used as a middle step in showing that the real matrices $M, \hat{M}$ are similar since they are each similar to $\left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right)$. Namely, we also have that $\left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right) = \begin{pmatrix} \hat{w}_1^1 & \hat{w}_2^1 \\ \hat{w}_1^2 & \hat{w}_2^2 \end{pmatrix}^{-1} \hat{M} \begin{pmatrix} \hat{w}_1^1 & \hat{w}_2^1 \\ \hat{w}_1^2 & \hat{w}_2^2 \end{pmatrix}$ where $\hat{w}_1, \hat{w}_2$ are the eigenvectors of $\hat{M}$ for the eigenvalues $i, -i$ respectively, where the notation of the coordinates of these vectors are analogous in the expected way to those for w_1, w_2. So, we see that $\begin{pmatrix} w_1^1 & w_2^1 \\ w_1^2 & w_2^2 \end{pmatrix}^{-1} M \begin{pmatrix} w_1^1 & w_2^1 \\ w_1^2 & w_2^2 \end{pmatrix} = \begin{pmatrix} \hat{w}_1^1 & \hat{w}_2^1 \\ \hat{w}_1^2 & \hat{w}_2^2 \end{pmatrix}^{-1} \hat{M} \begin{pmatrix} \hat{w}_1^1 & \hat{w}_2^1 \\ \hat{w}_1^2 & \hat{w}_2^2 \end{pmatrix}$ and thus $M = \left(\begin{pmatrix} \hat{w}_1^1 & \hat{w}_2^1 \\ \hat{w}_1^2 & \hat{w}_2^2 \end{pmatrix} \begin{pmatrix} w_1^1 & w_2^1 \\ w_1^2 & w_2^2 \end{pmatrix}^{-1} \right)^{-1} \hat{M} \left(\begin{pmatrix} \hat{w}_1^1 & \hat{w}_2^1 \\ \hat{w}_1^2 & \hat{w}_2^2 \end{pmatrix} \begin{pmatrix} w_1^1 & w_2^1 \\ w_1^2 & w_2^2 \end{pmatrix}^{-1} \right)$, meaning that M and $\hat{M}$ are indeed similar.

Finally, we show that any matrices $M, \hat{M} \in \mathrm{SL}_2(\mathbb{R})$ each with eigenvalue pair $(1, 1)$ that are not the identity are similar over $\mathrm{SL}_2(\mathbb{R})$. They are certainly each similar over $\mathbb{C}$ to its Jordan Normal Form $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. One might wonder how to find the basis such that M, when written in that basis, is exactly $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. The answer is through a simple, rote process of finding M generalized eigenvectors. Namely, an eigenvector v for an eigenvalue λ is one such that $(M - \lambda I)v = 0$ and a generalized eigenvector v is one such that $(M - \lambda I)^k v = 0$ for some $k \in \mathbb{N}_{\geq 2}$, and we call the smallest $k \in \mathbb{N}$ for which $(M - \lambda I)^k v = 0$ the order of the generalized eigenvector v. So, the first basis vector we need is simply an eigenvector u_1 for

the eigenvalue 1 and the second basis vector is a generalized eigenvector u_2 or order 2. Those are guaranteed to exist. At this point we simply construct our change of basis matrix P as the matrix with u_1, u_2 as its columns, and scale the first column appropriately so that the determinant of the resulting P is 0. Or put more precisely, $P = \begin{pmatrix} \frac{u_1^1}{u_1^1 u_2^2 - u_1^2 u_2^1} & u_2^1 \\ \frac{u_1^2}{u_1^1 u_2^2 - u_1^2 u_2^1} & u_2^2 \end{pmatrix}$. Then, $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) = P^{-1}MP$. Likewise, for $\hat{M}$ we have an associated $\hat{P} \in \mathrm{SL}_2(\mathbb{R})$ so that $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) = \hat{P}^{-1}\hat{M}\hat{P}$ and thus $M = (\hat{P}P^{-1})^{-1}\hat{M}(\hat{P}P^{-1})$.

So, $\mathrm{SL}_2(\mathbb{R})$ has four conjugacy classes, those with Jordan Normal Forms $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, and $\left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right)$ respectively.

3 Representation Theory

Question 3.1. *If you have a representation (θ, W) of H, a subgroup of a group G, how can you induce a representation of G?*

Let $L = \{L_i\}_{i \in [|G:H|]}$ be the set of left cosets of H in G. Then, note that any element of G has the form $g = l_{i_g} h_g$ where $l_{i_g} \in L_i$ belongs to a uniquely determined coset $L_i \in L$ and $h_g \in H$ is also uniquely determined. So, we let the induced representation $(\rho, \bigoplus_{L_i \in L} W)$ be defined by $\rho_g(\bigoplus_{L_i \in L} w_i) = \rho_{l_{i_g}}(\bigoplus_{L_i \in L} \theta_{h_g} w_i)$ where $\rho_{l_{i_g}}(\bigoplus_{L_i \in L} \theta_{h_g} w_i) = \bigoplus_{L_i \in L} \theta_{h_g} w_{j(i)}$ and $j = j(i) \in [|G : H|]$ is such that $L_i = l_{i_g} L_j$ or equivalently $L_j = l_{i_g}^{-1} L_i$.

Question 3.2. *If you have an irreducible representation of a subgroup, is the induced representation of the whole group still irreducible?*

No. Consider the permutation representation (ρ, V) of G on the set of left cosets G/H where V has basis $\{e_\alpha\}_{\alpha \in G/H}$ and $\rho_s e_\alpha = e_{s\alpha}$. Clearly, (ρ, V) is induced by the unit representation $e_H \subseteq V$ of H. However the permutation representation is not an irreducible representation of G since $span(\sum_{\alpha \in G/H} e_\alpha)$ is stable under the action of G due to the fact that left multiplication by any element $g \in G$ permutes left cosets.