# PhD Comprehensive Exam: Algebra Part II (nonspecialist) & Math 5055 Final Exam

Spring 2022

Solutions

**Your name:**

**Exam structure:**

There are 9 questions on this exam. The pass mark is 60%.

- The PhD comprehensive exam consists of all 9 questions.
- The Math 5055 final exam consists of the final 6 questions.

**Please indicate which exam you are taking.**

1. **Let $G$ be a group.**

   **(a) Give the definition of *subgroup* of $G$.**

   **(b) Prove that if $G$ is finite, then any nonempty subset of $G$ which is closed under multiplication is a subgroup.**

   **(c) Give an example to show that the conclusion in part (b) can fail if $G$ is infinite.**

   (a) **[7pts]** A subset $H \subset G$ is a subgroup if it is a group for the same operation. In other words, it must be closed under multiplication (if $g, h \in H$, then $gh \in H$) and contain the identity element and inverses ($1 \in H$ and if $h \in H$ then $h^{-1} \in H$). Note that associativity is inherited from the ambient group. Containing the identity follows from the other two for nonempty subsets.

   (b) **[8pts]** Suppose $H \subset G$ is nonempty and closed under multiplication. We must show that if $h \in H$, then so also $h^{-1} \in H$ (as then closure for multiplication implies that $1 = hh^{-1} \in H$). Since $G$ is finite, every $g \in G$ solves $g^{\#G} = 1$. Thus $h^{-1} = h^{\#G-1} = h \cdot h \cdot \cdots \cdot h$, which is contained in $H$ by the closure assumptions.

   (c) **[5pts]** For example, take $G = (\mathbb{Z}, +)$, the group of integers under addition, and $H = \mathbb{N} \subset G$. (There are many examples.)

2. **Let $G$ be a finite group and $p$ a prime. Suppose that $S, T \subset G$ are subgroups.**

   **(a) What does it mean for $S$ to be a *$p$-subgroup*? What does it mean for $S$ to be a *Sylow $p$-subgroup*?**

   **(b) Suppose that $S$ is a Sylow $p$-subgroup and $T$ is a $p$-subgroup. What can you say about the relationship between $S$ and $T$?**

   **(c) Suppose that $G = S_6$ is the symmetric group on 6 elements. How many Sylow 3-subgroups are there?**

   **(d) Suppose that $G$ has order $p^k \times m$ with $k \geq 1$ and $m < p$. Prove that $G$ is not simple.**

   (a) **[5pts]** A *$p$-subgroup* is a subgroup whose order is a power of $p$. It is *Sylow* if its index is coprime to $p$.

   (b) **[5pts]** All Sylow $p$-subgroups are conjugate, and all $p$-subgroups can be extended to Sylow $p$-subgroups. Thus $T$ is conjugate to a subgroup of $S$.

   (c) **[5pts]** An example of a Sylow 3-subgroup is $\langle (123), (456) \rangle$, and every other Sylow 3-subgroup is conjugate to this one. Thus the subgroup is uniquely determined by a choice of partition of $\{1, 2, 3, 4, 5, 6\}$ into two subsets each of size three. There are $\frac{1}{2}\binom{6}{3} = 10$ choices.

   (d) **[5pts]** The number of Sylow $p$-subgroups is $1 \pmod{p}$ and divides $m$. If $m < p$, then the only such number is 1. So there is a unique $p$-subgroup, and so that $p$-subgroup is normal.

3. **(a) How many (isomorphism classes of) abelian groups of order 300 are there? Justify your answer.**

   **(b) How many (isomorphism classes of) groups of order 10 are there? Justify your answer.**

(a) **[10pts]** The fundamental theorem of abelian groups says that every abelian group factors, uniquely up to isomorphism, into a product of cyclic groups of prime-power order. Since $300 = 2^2 \cdot 3 \cdot 5^2$, the factorizations are ($\mathbb{Z}_2^2$ or $\mathbb{Z}_4$) $\times$ ($\mathbb{Z}_3$) $\times$ ($\mathbb{Z}_5^2$ or $\mathbb{Z}_{25}$). So there are $2 \times 1 \times 2 = 4$ choices.

(b) **[10pts]** There are two such groups: the cyclic group $C_{10} = \mathbb{Z}_{10}$ and the dihedral group $D_{10}$. To prove this, let $G$ be a group of order 10. By Cauchy's theorem, $G$ contains an element $g$ of order 5. The cyclic subgroup $\langle g \rangle \subset G$ has order 5 and hence index 2 and so is normal. (Subgroups of index 2 are always normal.) The quotient group $G/\langle g \rangle$ has order 2. Since $G$ itself contains an element $h$ of order 2 (by Cauchy's theorem), $G$ arises as a semidirect product $\langle g \rangle \rtimes \langle h \rtimes$ — in other words, having chosen $g, h$, we can enumerate the elements of $G$ as $g^i h^j$ for $i \in \mathbb{Z}_5$ and $j \in \mathbb{Z}_2$. The group law on $G$ is fully determined by the value of $hg = g^i h$. Then $g \mapsto g^i$ is an automorphism of $\langle g \rangle \cong \mathbb{Z}_5$ of order 2. There are two such automorphisms: the trivial one ($i = 1$) and the nontrivial one ($i = 4$) [for example, the automorphism $\sigma : g \mapsto g^2$ does not have order 2, because $\sigma(\sigma(g)) = \sigma(g^2) = g^4 \neq g$].

4. **(a) Let $E$ be a field, and let $G \subset \mathrm{Aut}(E)$ be a set of field automorphisms of $E$. What does it mean to say that an element of $E$ is a *$G$-fixed point*?**

   **(b) Let $E^G \subset E$ denote the set of $G$-fixed points. Prove that $E^G \subset E$ is an extension of fields.**

   **(c) Give an example of an extension $F \subset E$ of fields such that $F \neq E^G$ for any set $G \subset \mathrm{Aut}(E)$ of field automorphisms.**

   (a) **[7pts]** By definition, the set of fixed points is $E^G = \{\alpha \in E | g\alpha = \alpha \, \forall g \in G\}$.

   (b) **[8pts]** The content is to prove that $E^G$ is a subfield of $E$. Certainly $0, 1 \in E^G$ since they are fixed by all automorphisms. Suppose $\alpha, \beta \in E^G$ (and assume $\beta \neq 0$ if necessary). Then for every $g \in G$, and for each of the field operations $\star \in \{+, -, \times, \div\}$, we have $g(\alpha \star \beta) = g\alpha \star g\beta = \alpha \star \beta$. It follows that $\alpha \star \beta \in E^G$, and so $E^G$ is a subfield of $E$. (The associativity, commutativity, and distributivity axioms are inherited from $E$.)

   (c) **[5pts]** For example, $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ and $\mathbb{Q} \subset \mathbb{R}$ both work, since the fields $\mathbb{Q}(\sqrt[3]{2})$ and $\mathbb{R}$ both have no nontrivial automorphisms. To compute $\mathrm{Aut}\,\mathbb{Q}(\sqrt[3]{2})$, note that any automorphism is determined by its action on $\sqrt[3]{2}$; its image must be a root of $x^3 - 2$. But this is the unique real root, and $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$. To compute $\mathrm{Aut}\,\mathbb{R}$, note that a number in $\mathbb{R}$ is positive if and only if it is a square, and so all automorphisms preserve the ordering on $\mathbb{R}$; but a real number is determined by the sets of rational numbers which are less than and greater than it.

5. **Let $\theta = \sqrt{3+\sqrt{11}}$.**

   **(a) Find the minimum polynomial $f$ of $\theta$ over $\mathbb{Q}$.**

   **(b) Let $K$ be the splitting field of $f$. Compute $\mathrm{Gal}(K/\mathbb{Q})$.**

   **(c) Find all intermediate subfields of $\mathbb{Q} \subset \mathbb{Q}(\theta)$.**

   **(d) Give an example of a transcendental extension of $\mathbb{Q}(\theta)$.**

   (a) **[3pts]** Note that $\theta^2 = 3+\sqrt{11}$, and so $(\theta^2-3)^2 = 11$, or in other words $\theta$ is a root of $f(x) = x^4 - 6x^2 - 2$. This polynomial is irreducible by Eisenstein's criterion with $p = 2$.

   (b) **[8pts]** Note that $\mathbb{Q}(\theta) \subset \mathbb{R}$ but $\theta' = \sqrt{3-\sqrt{11}}$ is an imaginary root of $f$. It follows that $K \supsetneq \mathbb{Q}(\theta)$. We know that $\mathbb{Q}(\theta)$ has degree 4 over $\mathbb{Q}$ and it is not hard to see that $K$ has degree at most 2 over $\mathbb{Q}(\theta)$. So $[K:\mathbb{Q}] = 8$. By the irreducibility of $f$, we can already conclude that $\mathrm{Gal}(K/\mathbb{Q}) = D_8$, since it is an order-8 subgroup of $S_4$.

   (c) **[7pts]** Other than $\mathbb{Q}$ and $\mathbb{Q}(\theta)$, the intermediate subfields of $\mathbb{Q}(\theta)$ are quadratic extensions of $\mathbb{Q}$ (since $[\mathbb{Q}(\theta):\mathbb{Q}] = 4$). We can see one option immediately: $\mathbb{Q}(\sqrt{11})$ is a subfield, since $\theta^2 - 3 = \sqrt{11} \in \mathbb{Q}(\theta)$. We claim that it is the only one. There are various ways to show this. A slow method is to compute the full lattice of subfields of $K$ (which is not what the question asks!). A quick method is to argue as follows. Suppose that there were another quadratic extension $\mathbb{Q}(\sqrt{a}) \subset \mathbb{Q}(\theta)$. Then $\mathbb{Q}(\sqrt{a},\sqrt{11})$ would have degree 4 over $\mathbb{Q}$ and be a subfield of $\mathbb{Q}(\theta)$ and hence equal to $\mathbb{Q}(\theta)$. But $\mathbb{Q} \subset \mathbb{Q}(\sqrt{a},\sqrt{11})$ is Galois whereas $\mathbb{Q} \subset \mathbb{Q}(\theta)$ is not.

   (d) **[2pts]** E.g. $\mathbb{Q}(\theta) \subset \mathbb{R}$.

6. **Let $\zeta_9$ be a primitive 9th root of unity.**

   **(a) Find the minimum polynomial $f$ of $\zeta_9$ over $\mathbb{Q}$.**

   **(b) Prove that $\mathbb{Q} \subset \mathbb{Q}(\zeta_9)$ is Galois. What is its Galois group?**

   **(c) Find all intermediate subfields of $\mathbb{Q} \subset \mathbb{Q}(\zeta_9)$. Describe these fields as simple extensions over $\mathbb{Q}$, i.e. give a single generator for each intermediate extension.**

(a) **[7pts]** $\zeta_9$ is a root of $x^9 - 1$, but that's not irreducible. Indeed, the 9th roots of unity are $\zeta_9^i$ for $i = \mathbb{Z}_9$, but only the $i \in \mathbb{Z}_9^\times = \{1, 2, 4, 5, 6, 7\}$ are primitive. The other three values $\zeta_9^3 = \zeta_3$, $\zeta_9^6 = \zeta_3^{-1}$, and $\zeta_9^9 = 1$ are roots of $x^3 - 1$. So the minimum polynomial is

$$f(x) = \prod_{i \in \mathbb{Z}_9^\times} (x - \zeta_9^i) = \frac{x^9 - 1}{x^3 - 1} = x^6 + x^3 + 1.$$

(b) **[5pts]** The other roots of $f$ are powers of $\zeta_9$, and so $\mathbb{Q}(\zeta_9)$ is the splitting field of $f$ over $\mathbb{Q}$. Since $f$ is separable (it has no repeated roots), $\mathbb{Q} \subset \mathbb{Q}(\zeta_9)$ is Galois. The Galois group is the copy of $\mathbb{Z}_9^\times$, where $i \in \mathbb{Z}_9^\times$ acts by $\zeta_9 \mapsto \zeta_9^i$. This Galois group is abelian of order 6 and hence isomorphic to $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$.

(c) **[8pts]** The subfields are indexed by the subgroups of $\mathbb{Z}_9^\times \cong \mathbb{Z}_6$. The latter description tells us to look for (the two improper subgroups and) exactly two proper subgroups, one of order 2 and the other of order 3. Thus, other than $\mathbb{Q}$ and $\mathbb{Q}(\zeta_9)$, we are looking for two subfields.

One is $\mathbb{Q}(\zeta_3)$, where $\zeta_3 = \zeta_9^3 = \frac{-1+\sqrt{-3}}{2}$ is a primitive cube root of unity. The extension $\mathbb{Q} \subset \mathbb{Q}(\zeta_3)$ is quadratic, and so this corresponds to the subgroup of $\mathbb{Z}_6$ of order 3.

Another is $\mathbb{Q}(\zeta_9) \cap \mathbb{R} = \mathbb{Q}(\zeta_9 + \zeta_9^{-1})$. This is a different subfield since $\zeta_3 \notin \mathbb{R}$. Note that $\zeta_9 + \zeta_9^{-1} = 2\cos 20°$ is famously algebraic of degree 3 over $\mathbb{Q}$, and so this extension corresponds to the subgroup of $\mathbb{Z}_6$ of order 2. (Indeed, that subgroup must consist of the identity and complex conjugation, and so the corresponding field must be $\mathbb{Q}(\zeta_9) \cap \mathbb{R}$. The only thing to check is that $\xi := \zeta_9 + \zeta_9^{-1} \notin \mathbb{Q}$. Well, $\xi^3 = \zeta_9^3 + \zeta_9^{-3} + 3(\zeta_9 + \zeta_9^{-1})$. But $\zeta_9^3 = \zeta_3$, and $\zeta_3 + \zeta_3^{-1} = -1$. So $\xi^3 = -1 + 3\xi$, which is to say $\xi$ is a root of $x^3 - 3x + 1$, which is irreducible by the rational root test.)

7. **Let $F$ be a field of characteristic $p > 0$.**

   **(a) What is the *Frobenius endomorphism* of $F$?**

   **(b) Prove that the Frobenius endomorphism is an automorphism if and only if every finite extension $F \subset E$ is separable.**

   **(c) Why does this imply that every extension of finite fields is separable?**

   **(d) Prove that if $F$ is a finite field, then $\mathrm{Aut}(F)$ is generated by the Frobenius endomorphism.**

(a) **[3pts]** The Frobenius endomorphism is the map $\phi : a \mapsto a^p$. It is manifestly multiplicative, and it is additive by the Frosh's Dream, and so it is a field endomorphism. We remark that field endomorphisms (indeed, field homomorphisms) are automatically injections.

(b) **[8pts]** As remarked already, $\phi$ is automatically an injection, and so it is an automorphism if and only if it is a surjection.

If $\phi$ is not surjective, pick $b$ not in its image. Let $E$ be the splitting field of $x^p - b$. This polynomial is purely inseparable — in $E$, all roots are equal, due for example to the injectivity of $\phi$ — and not $F$, and so $F \subset E$ is an inseparable extension.

Suppose that $\phi$ is surjective, and let $F \subset E$ be a finite extension. Given $\theta \in E$, let $f(x)$ be its minimal polynomial. Since $f$ is irreducible, if it were inseparable it would have to be of the form $f(x) = \sum_i a_i (x^p)^i$. Since $\phi$ is surjective, each $a_i = b_i^p$ for some $b_i$. Then $f(x) = (\sum_i b_i x^i)^p$, violating irreducibility.

(c) **[2pts]** Any injection from a finite set to itself is a bijection.

(d) **[7pts]** If $F$ is a finite field, then it is a finite extension of $\mathbb{F}_p$ for some positive prime $p$; let $n = [F : \mathbb{F}_p]$ be its index. Part of the fundamental theorem of Galois theory says that $\mathrm{Aut}(F)$ has order at most $n$, with equality when $\mathbb{F}_p \subset F$ is Galois. So it suffices to show that the Frobenius automorphism $\phi$ has order at least $n$ when acting on $F$.

Let $k > 0$. The fixed points of $\phi^k$ are the roots of $x^{p^k} - x$, of which there are at most $p^k$. If $k < n$, then $p^k < p^n$, and so not every element is fixed by $\phi^k$. Thus $\phi^k \neq \mathrm{id}$ if $k < n$.

8. **Find the Galois groups of the following polynomials over $\mathbb{Q}$ and over $\mathbb{R}$:**

**(a)** $x^3 - x^2 - 2x + 1$.
**Hint: The discriminant is** 49.

**(b)** $x^4 + 8x + 12$.
**Hint: The discriminant is** $331776 = 576^2$ **and the resolvent cubic is** $x^3 - 48x - 64$.

(a) **[10pts]**

**Over $\mathbb{Q}$:** We first check that $x^3 - x^2 - 2x + 1$ is irreducible. Since it is a cubic, it is irreducible as soon as it has no roots; by the rational root test, the rational roots must be factors of 1; neither $\pm 1$ is a root. Thus the Galois group over $\mathbb{Q}$ is a transitive subgroup of $S_3$. Since the discriminant is a square, the Galois group is a subgroup of $A_3$; and hence it is $A_3$.

**Over $\mathbb{R}$:** Since the discriminant is a square, the Galois group is a subgroup of $A_3$. It is not transitive since the cubic very definitely contains at least one real root. Thus the Galois group is trivial. (You can also show directly that this polynomial has three real roots, and so its splitting field over $\mathbb{R}$ is $\mathbb{R}$.)

(b) **[10pts]** Set $f(x) := x^4 + 8x + 12$.

**Over $\mathbb{Q}$:** We first check that $f$ is irreducible. It is monic, and so any rational roots are integers; but if $x$ is odd, then so is $f(x)$, whereas if $x$ is even, then $f(x) \cong 4 \pmod 8$. So $f$ does not have a linear factor. Can it have a quadratic factor? Reducing mod 5 gives $f(x) = x^4 + 3x + 2 \pmod 5$, and $f(-1) = 1 - 3 + 2 = 3 \pmod 5$. This means we can factor out a linear factor mod 5:

$$f(x) = (x + 1)(x^3 - x^2 + x + 2) \pmod 5.$$

If $f$ factored into a product of quadratics, then that factorization would descend mod 5. Since factorization in $\mathbb{F}_5[x]$ is unique, this would force $x^3 - x^2 + x + 2$ to have a quadratic factor mod 5, and hence to have a root mod 5. Checking all values mod 5 shows that it doesn't.

Thus the Galois group is a transitive subgroup of $S_4$, and in fact of $A_4$ since the discriminant is a square. It remains to decide if the Galois group is $A_4$ or $V = \mathbb{Z}_2^2$. This is decided by the resolvent cubic $g(x) = x^3 - 48x - 64$: either $g$ completely factors and the Galois group of $f$ is $V$, or $g$ is irreducible and the Galois group is $A_4$. Which is it? Since $g$ is cubic and monic, we just need to check if its roots are integers. Here is a fast check (there are slower methods): Note that $g'(x) = 3x^2 - 48$ has roots at $\pm 4$, so if there are three real roots, then one of them is between 4 and -4; but $g$ takes the values $64, 24, -27, -64$, at $x = -4, -3, -2, -1$, and so has a real but non integer root in this region; so $g$ does not completely factor and we decided already that either it completely factored or it was irreducible. As a result, $g$ is irreducible and the Galois group of $f$ is $A_4$.

**Over $\mathbb{R}$:** The derivative of $f$ is $f'(x) = 4x^3 + 8$, which has a unique real root (at $x = -\sqrt[3]{2}$). So $f$ cannot have four real roots, and its splitting field over $\mathbb{R}$ must be $\mathbb{C}$. The Galois group is thus $\mathbb{Z}/2$.

Note: $f(-\sqrt[3]{2}) = 2\sqrt[3]{2} - 8\sqrt[3]{2} + 12 = 12 - 6\sqrt[3]{2} > 0$, since $\sqrt[3]{2} < 2$. So $f$ takes only positive values, and so all roots are imaginary. In other words, $f$ factors over $\mathbb{R}$ as a product of two irreducible quadratics. Actually, this was forced by the Galois

group together with the descriminant: since the discriminant is a square, the Galois group is a subgroup of $A_4$; but the only order-2 element of $A_4$, up to conjugation, is $(12)(34)$.

9. **(a) What does it mean for a finite group to be *solvable*? Why is the word "solvable" used for this concept? What is it that can be "solved"?**

   **(b) Let $p$ be a prime. Prove that every finite $p$-group is solvable.**

   **(c) Give an example of an irreducible polynomial over $\mathbb{Q}$ of degree $5$ whose Galois group is solvable. Give an example of an irreducible polynomial over $\mathbb{Q}$ of degree $5$ whose Galois group is not solvable.**

(a) **[8pts]** A group $G$ is *solvable* if it can be built as an iterated extension of abelian (or equivalently of cyclic) groups. There are many equivalent conditions: for example, one can declare the definition inductively by saying that $G$ is solvable if it has an abelian normal subgroup with solvable quotient; or, again inductively, if it has a solvable normal subgroup with abelian quotient; or $G$ is solvable if its *derived series* (the sequence $G, G' = G^{(1)} = [G,G], G^{(2)} = (G^(1))', G^{(3)} = (G^{(2)})', \dots$) is eventually trivial.

The name comes because a polynomial is solvable in radicals (in the sense that its roots can be written in terms of the coefficients using just $+, -, \times, \div, \sqrt[n]{-}$) if and only if its Galois group is solvable.

(b) **[7pts]** A nontrivial $p$-group $G$ always has a nontrivial centre $Z(G)$, which is normal and abelian, and the quotient $G/Z(G)$ is solvable by induction on the order of $G$.

(c) **[5pts]** The polynomial $x^5 - 2$ is irreducible and its roots are manifestly given by radicals. (The splitting field is the degree-20 extension $\mathbb{Q}(\zeta_5, \sqrt[5]{2})$, and so the Galois group has order 20; the Sylow 5-subgroup is thus normal and cyclic hence abelian, and the quotient of order 4 is also abelian.)

The polynomial $x^5 - 100x + 2$ is irreducible by Eistenstein's criterion and has $3 = 5 - 2$ real roots; since 5 is prime, the Galois group must be $S_5$, which is not solvable. (Its only normal subgroup is $A_5$, which is in turn simple and nonabelian and hence not an extension of abelian groups.)