PhD Comprehensive Exam: Algebra Part II (nonspecialist) & Math 4055/5055 Final Exam

Spring 2024

Solutions

Your name:

Exam structure:

There are 9 questions on this exam. The pass mark is 70%.

- The PhD comprehensive exam consists of any 8 of the 9 questions. You have three hours to complete the comprehensive exam.
- The Math 4055/5055 final exam consists of any 6 of the 9 questions. You have two hours to complete the final exam.

Please indicate which exam you are taking.

1. Normal subgroups.

   (a) Give the definition of *subgroup*. Give the definition of *normal subgroup*. Give an example of a normal subgroup. Give an example of a subgroup which is not normal.

   (b) Show that any subgroup of index 2 is normal.

   Answers:

   (a) [6pt] If G is a group, a *subgroup* of G is a nonempty subset $H \subset G$ such that if $g, h \in H$, then $gh \in H$ and $g^{-1} \in H$. (Since H is nonempty, this implies that the identity element $e \in H$.) A subgroup $H \subset G$ is *normal* if for every $g \in G$ and every $h \in H$, ghg^{-1} is also in H. An example is the subgroup of S_3 generated by the permutation (123). A nonexample is the subgroup of S_3 generated by the permutation (12).

   (b) [4pt] Suppose that $H \subset G$ has index 2. This means that the quotient space G/H has order two. In other words, H has exactly two cosets: itself and $G \setminus H$. This is true for both left cosets and for right cosets: for every $g \in G$, we have $gH = Hg$ at the level of sets. This means that for every $h \in H$, we have $gh = h'g$ for some (unique but) possibly-different $h' \in H$. This $h' = ghg^{-1}$. So we see that H is normal.

2. The fundamental theorem of finite abelian groups.

   (a) List (up to isomorphism) all of the abelian groups of order 120. Explain/justify your answer.

   (b) List (up to isomorphism) all of the abelian groups of order 120 that are subgroups of the multiplicative group $F^\times$ of some field F. Explain/justify your answer.

   Answers:

   (a) [5pt] If A is a finite abelian group, then A factors canonically as $\prod_p A_{(p)}$, where p ranges over the primes and $A_{(p)}$ is the Sylow p-subgroup of A. (This is a version of the Chinese Remainder Theorem.) The order of $A_{(p)}$ is the p-part of the order of A. Factoring, we have $120 = 2^3 \times 3 \times 5$. Thus the groups $A_{(p)}$ for $p \geq 7$ are trivial, and $A_{(3)}$ and $A_{(5)}$ are cyclic of their respective orders and hence uniquely determined. The only question is the structure of the group $A_{(2)}$, which is abelian of order 8. The abelian groups of order 8 are indexed by the factorizations of 8: either cyclic ($8 = 8$) or a product of two cyclic groups ($8 = 4 \times 2$) or a product of three cyclic groups ($8 = 2 \times 2 \times 2$). Thus the final answer is:

   $$\mathbb{Z}/8\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}, \qquad \mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}, \qquad \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}.$$

   (b) [5pt] A finite subgroup of $F^\times$ is necessarily cyclic. This is because otherwise it would have too many elements of too-low order, and so the polynomial $x^n - 1$ (where n is that too-low order) would have too many solutions. Of the above groups, only one is cyclic:

   $$\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/120\mathbb{Z}.$$

3. Solvable groups.

   (a) When is a finite group *solvable*? Why is this name used?

   (b) When is a finite group *simple*? Why is this name used?

   (c) Suppose that $f(x) \in \mathbb{Q}[x]$ is irreducible of prime degree $p \geq 5$, and suppose that $f(x)$ has exactly $p-2$ real roots. Show that the roots of $f(x)$ cannot be expressed in terms of $+, -, \times, \div$, and $\sqrt[n]{-}$. You may use without proof that the alternating group A_p is simple, but you should explain how this is related to the problem.

Answers:

(a) [3pt] A finite group is *solvable* when it is an extension of cyclic groups: it has a normal abelian subgroup, and the quotient has a normal abelian subgroup, and so on, until you get to the trivial group. It is called this because a polynomial has solvable Galois group if and only it its roots are expressible in terms of $+, -, \times, \div$, and $\sqrt[n]{-}$ and the elements of the ground field.

(b) [3pt] A finite group is *simple* when it is not a nontrivial extension: it does not have any proper normal subgroups. It is called this because it cannot be broken up: its Jordan–Holder series is length one, which is as simple as they come.

(c) [4pt] Since f is irreducible, its Galois group G acts transitively on a set of order p. Thus $G \subset S_p$ has order divisible by p. So G contains a p-cycle. But G also contains complex conjugation, which is a 2-cycle. So $G = S_p$, since S_p is generated by any p-cycle together with any 2-cycle. But any subquotient of a solvable group is solvable, whereas $S_p \supset A_p$ which is simple. So S_p cannot be solvable, so f cannot be solved in radicals.

4. Splitting fields.

   (a) Give the definition of *degree* of a field extension. What is the degree of $\mathbb{Q} \subset \mathbb{Q}(\sqrt{7-\sqrt{2}})$? You do not need to justify your answer.

   (b) Give the definition of when $\mathbb{Q} \subset K$ is a *splitting* field of $\sqrt{7-\sqrt{2}}$. Show that if K is a splitting field of $\sqrt{7-\sqrt{2}}$, then $K \ni \sqrt{47}$.

   (c) What is the degree of a splitting field of $\sqrt{7-\sqrt{2}}$? You do not need to justify your answer.

   (d) What is the automorphism group of the field $\mathbb{Q}(\sqrt{7-\sqrt{2}})$? You do not need to justify your answer.

   (e) What is the automorphism group of a splitting field of $\sqrt{7-\sqrt{2}}$? You do not need to justify your answer.

   Answers:

   (a) [2pt] The *degree* of a field extension $F \subset E$ is the dimension of E over F. The degree of $\mathbb{Q} \subset \mathbb{Q}(\sqrt{7-\sqrt{2}})$ is 4.

   (b) [2pt] A *splitting field* of $\sqrt{7-\sqrt{2}}$ over $\mathbb{Q}$ is a field that contains, and is generated over $\mathbb{Q}$ by, all roots of the minimal polynomial of $\sqrt{7-\sqrt{2}}$. For example, the splitting field of $\sqrt{7-\sqrt{2}}$ would also contain $\sqrt{7+\sqrt{2}}$, and hence would contain

$$\sqrt{7-\sqrt{2}} \cdot \sqrt{7-\sqrt{2}} = \sqrt{7^2-2} = \sqrt{47}$$

   (c) [2pt] 8.

   (d) [2pt] $\mathbb{Z}/2\mathbb{Z}$.

   (e) [2pt] D_8.

5. Cyclotomic extensions and Galois correspondence.

   (a) Let ζ_{12} denote a primitive 12th root of unity. Show that $\mathbb{Q} \subset \mathbb{Q}(\zeta_{12})$ is Galois, and compute its Galois group. Also compute the minimal polynomial of ζ_{12}.

   (b) List all subfields of $\mathbb{Q}(\zeta_{12})$.

   Answers:

   (a) [5pt] All cyclotomic extensions are Galois, because they are splitting: the Galois conjugates of ζ_{12} are other primitive roots, and hence powers of ζ_{12}, and hence in $\mathbb{Q}(\zeta_{12})$. The Galois group is the $\mathrm{Aut}(\mathbb{Z}/12\mathbb{Z}) = (\mathbb{Z}/12\mathbb{Z})^\times = (\mathbb{Z}/4\mathbb{Z})^\times \times (\mathbb{Z}/3\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z})^2$.

   The minimal polynomial of ζ_{12} is thus of degree 4, and it suffices to find a degree-4 polynomial over $\mathbb{Q}$ that ζ_{12} solves. We have $\zeta_{12}^2 = \zeta_6$ and $\zeta_6 = \frac{1+\sqrt{-3}}{2}$ solves the equation $(2x-1)^2 + 3 = 0$. So ζ_{12} is a root of the polynomial

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

   or, dividing by 4,

   $$x^4 - x^2 + 1.$$

   (b) [5pt] There is a subfield of $\mathbb{Q}(\zeta_{12})$ for each subgroup of the Klein group $(\mathbb{Z}/2\mathbb{Z})^2$. This group has five subgroups: the trivial subgroups $\{0\}$ and $(\mathbb{Z}/2\mathbb{Z})^2$, corresponding respectively to $\mathbb{Q}(\zeta_{12})$, and three subgroups of order 2. These must correspond to quadratic extensions of $\mathbb{Q}$. One can work them out algorithmically, but it is also easy to eyeball three quadratic subfields of $\mathbb{Q}(\zeta_{12})$:

   $$\mathbb{Q}(\zeta_6) = \mathbb{Q}(\sqrt{-3}), \qquad \mathbb{Q}(\zeta_4) = \mathbb{Q}(\sqrt{-1}), \qquad \mathbb{Q}(\zeta_{12} + \bar{\zeta}_{12}) = \mathbb{Q}(\sqrt{3}).$$

6. Computing Galois groups.

   (a) Compute the Galois group of $x^3 - 7x + 5$ over $\mathbb{Q}$ and over $\mathbb{R}$.
   Hint: the discriminant is 697.

   (b) Compute the Galois group of $x^4 + 3x^2 + 3x - 3$ over $\mathbb{Q}$.
   Hint: the resolvent cubic is $x^3 - 3x^2 + 12x - 45$ and the discriminant is -35991.

Answers:

(a) [5pt] Let $f(x) = x^3 - 7x + 5$.

f is irreducible over $\mathbb{Q}$ by the rational root test, since a cubic is irreducible if and only if it has a root: the possible rational roots are ± 1 and ± 5, and $f(\pm 1) = \pm 1 \mp 7 + 5 \neq 0$ and $f(\pm 5) = \pm 125 \mp 35 + 5 \neq 0$. So the Galois group is either A_3 or S_3. The discriminant is not a square over $\mathbb{Q}$, and so the Galois group over $\mathbb{Q}$ is S_3.

f is reducible over $\mathbb{R}$, since all cubics are reducible over $\mathbb{R}$, so the Galois group is either trivial (A_2) or S_2. The discriminant is a square over $\mathbb{R}$, and so the Galois group over $\mathbb{R}$ is trivial.

(b) [5pt] Let $f(x) = x^4 + 3x^2 + 3x - 3$ and $g(x) = x^3 - 3x^2 + 12x - 45$.

f is irreducible over $\mathbb{Q}$ by Eisenstein's criterion (with $p = 3$), so the Galois group over $\mathbb{Q}$ is a transitive subgroup of S_4.

Note that $g'(x) = 3x^2 + 6x^2 + 12 = 3(x^2 + 2x + 4)$, which has no real roots, since $2^2 - 4 \times 4 \times 1 < 0$. So g has exactly one real root. Testing some values, we see that

$$g(3) = 27 - 27 + 36 - 45 = -9 < 0, \qquad g(4) = 64 - 36 + 48 - 45 = 31 > 0.$$

So the unique real root of g is not an integer, and so g is irreducible over $\mathbb{Q}$. It follows that the Galois group of g over $\mathbb{Q}$ contains a 3-cycle, and hence this is also true for the Galois group of f. So the Galois group of f is either S_4 or A_4.

The discriminant is negative and hence not a square. So the Galois group of f over $\mathbb{Q}$ is S_4.

7. Finite fields.

   (a) Recall that $\mathbb{F}_{27}$ is generated, as a field, by a single element. How many elements of $\mathbb{F}_{27}$ are generators of $\mathbb{F}_{27}$ as a field?

   (b) Recall that $\mathbb{F}_{27}^\times$ is generated, as a group, by a single element. How many elements of $\mathbb{F}_{27}^\times$ are generators of $\mathbb{F}_{27}^\times$ as a group?

   (c) How many field automorphisms does $\mathbb{F}_{27}$ have? Into how many orbits does the set from question (7a) break under the action of $\mathrm{Aut}(\mathbb{F}_{27})$? What about the set from question (7b)?

   (d) Find the minimal polynomial of some element that generates $\mathbb{F}_{27}^\times$ as a group. (Hint: there is more than one answer.) Justify your answer.

Answers:

(a) [1pt] The only subfields of $\mathbb{F}_{27}$ is $\mathbb{F}_3$. So $\mathbb{F}_{27}$ has $27 - 3 = 24$ generators as a field.

(b) [2pt] The group $\mathbb{F}_{27}^\times$ is cyclic of order $26 = 2^1 \times 13^1$, and so has $(2^1 - 2^0) \times (13^1 - 13^0) = 12$ generators as a group.

(c) [3pt] Since $27 = 3^3$, the Galois group of $\mathbb{F}_{27}$ over $\mathbb{F}_3$ is cyclic of order 3. It acts on the sets from parts (7a) and (7b) without stabilizer. So it splits the 24 field generators into $24/3 = 8$ orbits, and it splits the 12 group generators into $12/3 = 4$ orbits.

(d) [4pt] An element $\alpha \in \mathbb{F}_{27}$ generates $\mathbb{F}_{27}^\times$ as a group iff $\alpha \notin \mathbb{F}_3$ (and hence $\alpha^2 \neq 1$) and also $\alpha^{13} \neq 1$. But $\alpha^{26} = 1$, so $\alpha^{13} = -1$. So we simply need to find an irreducible cubic over $\mathbb{F}_3$ that divides $x^{13} + 1$. We could work systematically, but a faster method is to guess and check. Recall that a cubic is irreducible as soon as it has no roots, and that $x^3 - x$ takes constant value 0 on $\mathbb{F}_3$, so that $x^3 - x \pm 1$ takes constant value ± 1 and hence is irreducible. Let's see if either of those answers work.

We could do this by long division, but since we don't actually care about the quotient, only the remainder, we can do it even faster. What we want is to know: What is the remainder of x^{13} upon division by $x^3 - x \pm 1$? (We want the answer to be "-1.") Note that $x^3 \equiv x \mp 1$, and so

$$x^{12} = (x^3)^4 \equiv (x \mp 1)^4 = x^4 \mp 4x^3 + 6x^2 \mp 4x + 1 = x^4 \mp x^3 \mp x + 1$$

since we are working mod 3. This simplifies further to

$$= x^3(x \mp 1) \mp x + 1 \equiv (x \mp 1)^2 \mp x + 1 = x^2 \pm x + 1 \mp x + 1 = x^2 - 1.$$

Multiplying by x gives:

$$x^{13} \equiv x^3 - x = x \mp 1 - x = \mp 1.$$

We want the answer to be -1. So we find that $\boxed{x^3 - x + 1}$ works.

8. The Frobenius map and inseparable extensions.

   (a) Let F be a field of positive characteristic. Define the *Frobenius endomorphism* $\mathrm{Frob}_F : F \to F$.

   (b) Give an example of a field F such that Frob_F is an automorphism.

   (c) Give an example of a field F such that Frob_F is a not an automorphism.

   (d) Give definitions of the following terms:

   - (in)separable polynomial
   - (in)separable extension
   - perfect field

   (e) State without proof the relationship between whether F is perfect and whether Frob_F is an automorphism.

   Answers:

   (a) [2pt] If F has characteristic p, then $\mathrm{Frob}_F : F \to F$ is the map $\alpha \mapsto \alpha^p$.

   (b) [2pt] An example with Frob_F an automorphism is $F = \mathbb{F}_p$, or more generally any finite field.

   (c) [2pt] An example with Frob_F an non-automorphism is $F = \mathbb{F}_p(x)$. The element x is not in the range of Frop_F.

   (d) [2pt] A polynomial $p(x)$ is *separable* if it has no repeated roots, equivalently if it is coprime to its derivative; otherwise $p(x)$ is *inseparable*. A field extension $F \subset E$ is *separable* if it is algebraic and the minimal polynomial (over F) of every element of E is separable; a field extension $F \subset E$ is *inseparable* if it is algebraic but not separable. A field F is *perfect* if all of its algebraic extensions are separable.

   (e) [2pt] A positive-characteristic field F is perfect if and only if Frob_F is an automorphism. (Fields of characteristic zero are always perfect.)

9. Transcendental extensions.

   (a) What does it mean to say that a field extension $F \subset E$ is *transcendental*? Give an example of a transcendental extension.

   (b) Suppose that $F \subset E$ is a field extension. What does it mean that a subset $S \subset E$ is a *transcendence base* for E over F?

   (c) Show that any nontrivial field extension of $\mathbb{C}$ has uncountable dimension.

   Answers:

   (a) [2pt] $F \subset E$ is *transcendental* if there is some element $\alpha \in E$ such that the evaluation map $F[x] \to E$ sending $x \mapsto \alpha$ is injective (and hence extends to the field of rational functions $F(x) \to E$). Examples include $F \subset F(x)$ and $\mathbb{Q} \subset \mathbb{R}$.

   (b) [2pt] A subset $S \subset E$ is called a *transcendence base* over F if it is:

   - Independent: the elements of S do not satisfy any nontrivial polynomial identity over F. More precisely, for any finite subset $s_1, \ldots, s_n$, the map $F[x_1, \ldots, x_n] \to E$ sending $x_i \mapsto s_i$ is an injection (and hence extends to the field of rational functions $F(x_1, \ldots, x_n)$).
   - Spanning: the elements of S generate E up to algebraic extensions. More precisely, writing $F(S)$ for the subfield of E generated by $F \cup S$, the extension $F(S) \subset E$ should be algebraic.

   (c) [6pt] Since $\mathbb{C}$ is algebraically closed, any nontrivial field extension of it must be transcendental. Thus it suffices to show that $\dim_{\mathbb{C}} \mathbb{C}(x)$ is uncountable. But the elements $\frac{1}{x-\lambda}$ for $\lambda \in \mathbb{C}$ are linearly independent, and there are uncountably many of them.