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

Spring 2022

Solutions to sample exam

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

   (a) What does it mean to say that a subgroup $K \subset G$ is *normal*?

   (b) Suppose that $H \subset G$ is a subgroup, and $K \subset G$ is a normal subgroup. Show that the *product*

   $$HK := \{hk | h \in H, k \in K\}$$

   is a subgroup of G.

(a) A subgroup $K \subset G$ is *normal* if it is preserved by inner automorphisms of G. Spelled out, this means that if $k \in K$ and $g \in G$, then $gkg^{-1} \in K$.

(b) HK contains $1 = 1 \cdot 1$, since $1 \in H$ and $1 \in K$.

Suppose that $h_1k_1, h_2k_2 \in HK$. Then

$$h_1k_1h_2k_2 = (h_1h_2)((h_2^{-1}k_1h_2)k_2).$$

Note that $h_2^{-1}k_1h_2 \in K$ (take $g = h_2^{-1}$ in part (a)), and so $h_1h_2 \in H$ and $(h_2^{-1}k_1h_2)k_2 \in K$. So HK is closed under multiplication.

Given $hk \in HK$, compute

$$(hk)^{-1} = k^{-1}h^{-1} = (h^{-1})(hk^{-1}h^{-1}).$$

But $hk^{-1}h^{-1} \in K$ since K is normal (and $h^{-1} \in H$ since H is a subgroup).

2. **Let G be a finite group.**

   (a) Define the *centre* $Z(G)$ of G and the *derived subgroup* $G' = [G, G]$ of G.

   (b) Show that both $Z(G)$ and G' are normal subgroups of G.

   (c) Let p be a prime. Show that if G is nonabelian of order p^3, then $Z(G) = G'$.

   (d) Show that if G is nonabelian of order 6, then $Z(G) \neq G'$.

   (a) The *center* is $Z(G) = \{g \in G | gh = hg \, \forall h \in G\}$.
   The *derived subgroup* is the subgroup generated by elements of the form $ghg^{-1}h^{-1}$. It is the smallest normal subgroup $N \subset G$ such that N/G is abelian.

   (b) A subgroup is *normal* if it is preserved by all inner automorphisms. These subgroups are better than normal: they are *characteristic*, meaning that they are preserved by all automorphisms. Indeed, this is manifest: the definitions of $Z(G)$ and G' are obviously isomorphism-invariant.

   (c) This was part of a homework problem. If G is has order p^3, then it contains a nontrivial centre. If G is nonabelian, then $G/Z(G)$ is nontrivial. So $G/Z(G)$ has order either p or p^2, and hence is abelian. Thus $G' \subset Z(G)$, since G' is the smallest subgroup for which the quotient is abelian. Again using that since G is nonabelian, we know that $G' \neq \{1\}$. So it suffices to show that $Z(G)$ has exact order p. Suppose for contradiction that $Z(G)$ had order p^2, and choose any element $x \in G \setminus Z(G)$. Then the p^3 many elements zx^i where z ranges over $Z(G)$ and i ranges from 0 to $p - 1$ would be all distinct. But they all commute with each other, contradicting the nonabelianness of G.

   (d) The derived subgroup has order three, whereas the centre is trivial.

3. **Prove that there is no simple group of order** $980 = 2^2 \times 5 \times 7^2$**. Hint: Constrain the number of Sylow subgroups.**

   The number of Sylow p-subgroups is $1 \pmod{p}$ and divides the index of a Sylow p-subgroup. In particular, the number of Sylow 2-subgroups is odd and divides 5×7^2 (not very useful); the number of Sylow 5-subgroups is $1 \pmod{5}$ and divides $196 = 2^2 \times 7^2$, and so is either 1 or 196; and the number of Sylow 7-subgroups is $1 \pmod{7}$ and divides 20. Aha! The only factor of 20 which is $1 \pmod{7}$ is 1 itself, so there is a unique Sylow 7-subgroup, which is then necessarily normal.

4. **(a) What does it mean for a field extension $F \subset E$ to have *degree* n?**

   (b) Prove that if $F \subset E$ has degree $n < \infty$, then every element of E is a root of some polynomial over F of degree $\leq n$.

   (c) State, but do not prove, a relationship between the degree of $F \subset E$ and the order of $\mathrm{Gal}(E/F)$.

   (a) If $F \subset E$ is a field extension, then the multiplication makes E into an F-vector space. The *degree* is its dimension:
   $$[E : F] = \dim_F E.$$

   (b) Suppose $[E : F] = n < \infty$. Given $\alpha \in E$, the list $1, \alpha, \alpha^2, \ldots, \alpha^n \in E$ has length $n + 1 > \dim E$, and so must admit a nontrivial linear dependency. But this dependency *is* a polynomial equation satisfied by α.

   (c) $[E : F] \geq \#\,\mathrm{Gal}(E/F)$.

5. **Consider the field extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{5}, \sqrt{7})$.**

   (a) Is this extension Galois?

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

   (c) Give an example of a transcendental extension of $\mathbb{Q}(\sqrt{2}, \sqrt{5}, \sqrt{7})$.

(a) Yes, this extension is Galois. The Galois group is $(\mathbb{Z}/2)^3$ consisting of the sign flips of subsets of the generators. (For example, there is a unique automorphism taking $\sqrt{2} \mapsto -\sqrt{2}$, $\sqrt{5} \mapsto -\sqrt{5}$, and $\sqrt{7} \mapsto \sqrt{7}$.)

(b) The subfields are in bijection with the subgroups of $(\mathbb{Z}/2)^3$.

The trivial subgroup corresponds to $\mathbb{Q}(\sqrt{2}, \sqrt{5}, \sqrt{7})$ itself. It can be generated by the single element $\sqrt{2} + \sqrt{5} + \sqrt{7}$.

There are seven subgroups of order 2. These correspond to quartic extensions of $\mathbb{Q}$:

- Three of these subgroups flip the sign of a single $\sqrt{a}$, where $a \in \{2, 5, 7\}$. The corresponding field is $\mathbb{Q}(\sqrt{b} + \sqrt{c})$, where $\{b, c\} = \{2, 5, 7\} \setminus \{a\}$.
- Three of these subgroups act as $\sqrt{a} \mapsto -\sqrt{a}$, $\sqrt{b} \mapsto -\sqrt{b}$, $\sqrt{c} \mapsto \sqrt{c}$, where $\{a, b, c\} = \{2, 5, 7\}$. The corresponding fields are $\mathbb{Q}(\sqrt{c} + \sqrt{ab})$.
- One order-2 subgroup flips the signs of all three generators. The corresponding field is $\mathbb{Q}(\sqrt{10} + \sqrt{14}) = \mathbb{Q}(\sqrt{10} + \sqrt{35}) = \mathbb{Q}(\sqrt{14} + \sqrt{35})$.

The are also seven subgroups of order 4. These correspond to quadratic extensions $\mathbb{Q}(\sqrt{m})$ where $m \in \{2, 5, 7, 10, 14, 35, 70\}$.

Finally, the subgroup of the Galois group of order 8 corresponds to the field $\mathbb{Q} = \mathbb{Q}(1)$.

(c) For example, $\mathbb{R}, \mathbb{C}, \mathbb{Q}(\sqrt{2}, \sqrt{5}, \sqrt{7}, \pi), \ldots$.

6. **Set** $F = \mathbb{Q}(\sqrt{7})$**, and set** $K_1 = F(\sqrt{2+\sqrt{7}})$ **and** $K_2 = F(\sqrt{2-\sqrt{7}})$**. Let** $E = K_1K_2$ **be the composite field.**

   (a) Which of the following extensions are Galois?

$$\mathbb{Q} \subset F, \qquad \mathbb{Q} \subset K_1, \qquad \mathbb{Q} \subset K_2, \qquad \mathbb{Q} \subset E,$$
$$F \subset K_1, \qquad F \subset K_2, \qquad F \subset E, \qquad K_1 \subset E, \qquad K_2 \subset E$$

   (b) For the extensions in part (a) which are Galois, what is the Galois group?

We remark that $K_1 \subset \mathbb{R}$ whereas $K_2 \not\subset \mathbb{R}$, and so $K_1 \neq K_2$. On the other hand, $K_1 \cong K_2$ are isomorphic (lifting the automorphism $\sqrt{7} \mapsto -\sqrt{7}$ of F).

The extensions $\mathbb{Q} \subset F, F \subset K_1, F \subset K_2, K_1 \subset E, K_2 \subset E$ are all quadratic and hence Galois with Galois group $\mathbb{Z}/2$.

The extension $F \subset E$ is splitting and hence Galois (since we are in characteristic 0). Its degree is 4, and it contains the inequivalent subfields K_1, K_2, and so the Galois group is $V = (\mathbb{Z}/2)^2$ (and not $\mathbb{Z}/4$).

The extensions $\mathbb{Q} \subset K_1, K_2$ are not Galois. Indeed, the automorphism of F does not extend to an automorphism of either K_1 or K_2 (but rather to an isomorphism between them) and so K_1, K_2 are not splitting.

The extension $\mathbb{Q} \subset E$ is Galois, since E is the splitting field of the minimal polynomial of $\sqrt{2+\sqrt{7}}$. The Galois group is an order-8 subgroup of S_4, and hence dihedral of order 8.

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

   (a) $x^3 + 3x^2 + 2x - 1$.
   Hint: The discriminant is -23.

   (b) $x^4 - 4x^2 + x + 1$.
   Hint: The discriminant is 1957 and the resolvent cubic is $x^3 + 4x^2 - 4x + 15$.

(a) This polynomial is irreducible over $\mathbb{Q}$ by the rational root test: if it were reducible, then one factor would be linear, and so it would have a rational, hence integral, root, which would necessarily divide 1; but neither ± 1 is a root. The discriminant is not a square, so the Galois group is S_3.

Over $\mathbb{R}$, the discriminant is not a square but the polynomial does have a root. So there is a unique real root, the splitting field is $\mathbb{C}$, and the Galois group is $\mathbb{Z}/2$.

(b) This polynomial is irreducible over $\mathbb{Q}$. To see this, note first that it does not have a rational root (which would necessarily be ± 1). Suppose that it factored as a product of quadratics. Then it would factor over $\mathbb{Z}$, and hence factor into a product of quadratics over $\mathbb{Z}/3 = \mathbb{F}_3$. But working mod 3 we have

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

and $x^3 - x + 1$ is irreducible over $\mathbb{F}_3$ (since it doesn't have a root). But factorization of polynomials over $\mathbb{F}_3$ (or any field) is unique.

The discriminant $1957 = 19 \times 103$ is not a square in $\mathbb{Q}$. Furthermore, the resolvent cubic is irreducible over $\mathbb{Q}$: if it were reducible, it would have a root which would divide 15 and be divisible by 3 (since the cubic is $x^3 + x^2 - x \pmod 3$), and direct checking rules out $\pm 3, \pm 15$. So the Galois group over $\mathbb{Q}$ is S_4.

Over $\mathbb{R}$, this quartic polynomial factors completely. Indeed, it takes the values

x	$x^4 - 4x^2 + x + 1$
$-\infty$	$+\infty$
-1	-3
0	1
1	-1
$+\infty$	$+\infty$

and so must have at least four real roots. So the Galois group is trivial.

8. **(a) What does it mean for a field extension $F \subset E$ to be *separable*?**

   (b) What does it mean for a field extension $F \subset E$ to be *purely inseparable*?

   (c) Give an example of a nontrivial field extension which is purely inseparable.

   (d) Give an example of a nontrivial field extension which is neither separable nor purely inseparable.

(a,b) A polynomial $f(x) \in F[x]$ is *separable* if it has no repeated roots (in any field extension), or equivalently if $f(x)$ and the derivative $f'(x) = \frac{\mathrm{d}f}{\mathrm{d}x}$ are relatively prime. It is *purely inseparable* if it has only one root in any field extension, i.e. if after a field extension $f(x) = (x - \alpha)^n$.

A field extension $F \subset E$ is *separable*, resp. *purely inseparable*, if it is algebraic and furthermore for every $\alpha \in E$, the minimal polynomial of α over F is separable, resp. purely inseparable.

(c) An example of a nontrivial purely inseparable extension is to start with a field K of characteristic p, set $F = K(t)$, the field of Laurent polynomials in one variable, and set $E = F(\sqrt[p]{t})$.

(d) An example which is neither separable nor purely inseparable, take $F = K(t)$ as in part (c), but take $E = F(\sqrt[m]{t})$ where m is divisible by p but not a power of p.

9. **(a) Suppose that F is field. Prove that if $G \subset F^\times$ is a finite subgroup, then G is cyclic. Conclude that if F is finite, then $\mathbb{F}^\times$ is cyclic.**

   (b) Describe the group $\mathbb{C}^\times$.

   (c) Prove that for each prime p and each positive integer n, there exists a field $\mathbb{F}_{p^n}$ of order p^n, and that it is unique up to isomorphism.

   (a) Suppose for contradiction that G is not cyclic. Because G is abelian, if it is finite then it factors into a product of cyclic groups; if it is not cyclic, then G must contain a subgroup isomorphic to $(\mathbb{Z}/p)^2$ for some prime p. But then the polynomial $x^p - 1$ would have at least p^2 roots in F.

   (b) This (infinite!) group is isomorphic to $\mathbb{R} \times S^1$, where $S^1 = \mathrm{U}(1)$ is the circle group. The isomorphism is given by polar coordinates: $(r, \theta) \mapsto r \times e^{i\theta}$. There are plenty of subgroups which cannot be generated by a single generator, for example the subgroup consisting of complex numbers of the form $2^a \times e^{ib}$ for $a, b \in \mathbb{Z}$. (This subgroup is isomorphic to $\mathbb{Z}^2$. That it is not a quotient of $\mathbb{Z}^2$ follows immediately from the irrationality of π.)

   (c) Suppose that there is such a field. Then $\mathbb{F}_{p^n}^\times$ is cyclic of order $N = p^n - 1$. Then this field completely splits the polynomial $x^N - 1 \in \mathbb{F}_p[x]$. So if $\mathbb{F}_{p^n}$ exists, then it is said splitting field, confirming uniqueness.

   It suffices to show that the splitting field of $x^N - 1$, or equivalently of $x^{p^n} - x$, contains precisely p^n elements. Equivalently, it suffices to show that the solutions to $x^{p^n} = x$ are a field. They are obviously closed under multiplication, and closure under addition follows from the *Frosh's Dream* — the statement that, in characteristic p, $(x + y)^p = x^p + y^p$.