

# Algebra Qualifying Exams

---

## Spring 2016

1. (a) Prove that every subgroup of a cyclic group is cyclic.

*Proof.* Let  $G$  be a cyclic group. First, suppose that  $G$  is of infinite order. Then sending the generator of  $G$  to  $1 \in \mathbb{Z}$  gives an isomorphism  $G \cong \mathbb{Z}$ . We claim that every subgroup of  $\mathbb{Z}$  is of the form  $n\mathbb{Z}$ , which is clearly cyclic. Let  $H$  be a subgroup of  $G$  and let  $n$  be the smallest positive integer in  $H$ . Then  $n\mathbb{Z} \subseteq H$ . Suppose the containment is strict and let  $m$  be the smallest positive integer in  $H \setminus n\mathbb{Z}$ . We then have that  $1 \leq \gcd(m, n) < n$  and by Bezout's identity we have that  $\gcd(m, n) = um + vn$  for some  $u, v \in \mathbb{Z}$  is in  $H$ . But this contradicts the minimality of  $n$ , so we conclude that  $H = n\mathbb{Z}$ .

Suppose now that  $G = \langle g \rangle$  is finite of order  $n$  so that  $G \cong \mathbb{Z}/n\mathbb{Z}$ . By the fourth isomorphism theorem (or lattice/correspondence theorem) there is a one-to-one correspondence between subgroups of  $\mathbb{Z}/n\mathbb{Z}$  and subgroups of  $\mathbb{Z}$  containing  $n\mathbb{Z}$ . We have already shown that all subgroups of  $\mathbb{Z}$  are cyclic, and since the homomorphic image of a cyclic group is cyclic ( $\varphi(g^k) = \varphi(g)^k$ ), we have that all subgroups of  $\mathbb{Z}/n\mathbb{Z}$  are cyclic.  $\square$

- (b) Is the automorphism group of a cyclic group necessarily cyclic?

*Solution.* This need not be the case. Let  $G \cong \mathbb{Z}/N\mathbb{Z}$ . As  $G$  is cyclic, any automorphism of  $G$  is determined by where it sends a generator and it must map a generator to a generator. The generators of  $\mathbb{Z}/N\mathbb{Z}$  exactly correspond to the elements of  $(\mathbb{Z}/N\mathbb{Z})^\times$  and we have that  $\text{Aut}(\mathbb{Z}/N\mathbb{Z}) \cong (\mathbb{Z}/N\mathbb{Z})^\times$ . If  $N$  is a product of distinct primes  $p, q > 2$  then the Chinese remainder theorem says that

$$(\mathbb{Z}/N\mathbb{Z})^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/(q-1)\mathbb{Z},$$

which is not cyclic  $\square$

2. Let  $G = \mathbb{Z}/25\mathbb{Z}$  be the cyclic group of order 25.

- (a) Can  $G$  be given the structure of a  $\mathbb{Z}[i]$ -module?

*Solution.* Yes it can. Observe that in  $\mathbb{Z}/25\mathbb{Z}$ ,  $-1 = 24 = 6 \cdot 4 = 9^2 \cdot 2^2$ , so  $18^2 = -1$ . Define the action of  $a + bi \in \mathbb{Z}[i]$  on  $m \in \mathbb{Z}/25\mathbb{Z}$  by

$$(a + bi) \cdot m = (a + 18b)m.$$

This action gives  $G$  the structure of a  $\mathbb{Z}[i]$ -module since

$$\begin{aligned}
[(a + bi) + (c + di)] \cdot m &= [(a + c) + (b + d)i] \cdot m \\
&= [(a + c) + 18(b + d)]m \\
&= (a + bi) \cdot m + (c + di) \cdot m. \\
(a + bi) \cdot (m + n) &= (a + 18b)(m + n) \\
&= (a + bi) \cdot m + (a + bi) \cdot n. \\
[(a + bi)(c + di)] \cdot m &= [(ac - bd) + (ad + bc)i]m \\
&= [(ac - bd) + 18(ad + bc)]m \\
&= (a + bi) \cdot [(c + di) \cdot m].
\end{aligned}$$

□

(b) Can  $G$  be given the structure of a  $\mathbb{Z}/5\mathbb{Z}$  module?

*Solution.* No it cannot. If it could then we would have

$$\begin{aligned}
0 &= 0 \cdot 1 \\
&= 5 \cdot 1 \\
&= (1 + 1 + 1 + 1 + 1) \cdot 1 \\
&= 1 \cdot 1 + 1 \cdot 1 + 1 \cdot 1 + 1 \cdot 1 + 1 \cdot 1 \\
&= 5 \\
&\neq 0.
\end{aligned}$$

□

3. Prove that there is no simple group of order 520.

*Proof.* Write  $520 = 2^3 \cdot 5 \cdot 13$ . By Sylow's theorems, the number of Sylow-5 subgroups,  $n_5$  is 1 mod 5 and divides  $2^3 \cdot 13 = 104$ . The only positive integers satisfying these constraints are 1 and 26. The same reasoning shows that  $n_{13}$  must be 1 or 40. If either of  $n_5$  or  $n_{13}$  is 1, then since Sylow- $p$  subgroups are conjugate to one another, then that subgroup would be normal. Suppose then that  $n_5 = 26$  and  $n_{13} = 40$ . Then there are  $26 \cdot 4 = 104$  elements of order 5 and  $40 \cdot 12 = 480$  elements of order 13. But  $104 + 480 = 584 > 520$ , so this cannot be the case. We conclude that there must be a unique Sylow-5 or Sylow-13 subgroup which is normal. □

4. Let  $G$  be a finite group acting transitively on a set  $X$  with  $|X| > 1$ .

(a) State the orbit-stabilizer theorem.

*Solution.* If a group  $G$  acts on a set  $X$  then for any  $x \in X$ , the size of the orbit of  $x$  under  $G$  is the index of the stabilizer of  $x$  under  $G$ ,  $|\mathcal{O}(x)| = [G : \text{Stab}(x)]$ .  $\square$

(b) Show that there is some element of  $G$  fixing no element of  $X$ .

*Proof.* Since the action of  $G$  on  $X$  is transitive there is a single orbit. Burnside's lemma (which immediately follows from the orbit-stabilizer theorem) then states that

$$1 = \frac{1}{|G|} \sum_{g \in G} |\{x \in X : g \cdot x = x\}|.$$

If  $g \in G$  has fixed points then it contributes at least  $1/|G|$  to the above sum. If *every* element has a fixed point then we must have that every term in the sum is  $1/|G|$ . But the identity element fixes every element in  $X$  and  $|X| > 1$ , so we must have that one term in this sum is zero, i.e. at least one element of  $G$  is fixed point free.  $\square$

5. Let  $K$  be a field and let  $\bar{K}$  be an algebraic closure of  $K$ . Assume  $\alpha, \beta \in \bar{K}$  have degree 2 and 3 over  $K$ , respectively.

(a) Can  $\alpha\beta$  have degree 5 over  $K$ ?

*Solution.* No it cannot. We have that  $K(\alpha\beta)$  is contained in the composite extension  $K(\alpha)K(\beta)$ . Furthermore, since the degrees of  $K(\alpha)$  and  $K(\beta)$  over  $K$  are relatively prime, we have that the composite extension has degree 6 over  $K$ . Since  $K(\alpha\beta)$  is a subfield of the composite extension, its degree over  $K$  must divide 6. Since 5 doesn't divide 6 we have that  $K(\alpha\beta)$  cannot have degree 5 over  $K$ .  $\square$

(b) Can  $\alpha\beta$  have degree 6 over  $K$ ?

*Solution.* Yes it can. Consider  $\mathbb{Q}(\sqrt{2})$  and  $\mathbb{Q}(\sqrt[3]{2})$ .  $x^2 - 2$  and  $x^3 - 2$  are irreducible over  $\mathbb{Q}$  by Eisenstein so these extensions are of degree 2 and 3, respectively. We claim that the product  $2^{1/2} \cdot 2^{1/3} = 2^{5/6}$  has degree 6 over  $\mathbb{Q}$ .

We start by showing that  $\mathbb{Q}(2^{5/6}) = \mathbb{Q}(2^{1/6})$ . Clearly  $\mathbb{Q}(2^{5/6}) \subseteq \mathbb{Q}(2^{1/6})$ . On the other hand,  $\frac{1}{24}(2^{5/6})^5 = 2^{1/6}$ , so  $\mathbb{Q}(2^{1/6}) \subseteq \mathbb{Q}(2^{5/6})$ . Finally,  $2^{1/6}$  is a root of the polynomial  $x^6 - 2$ , which is irreducible over  $\mathbb{Q}$  by Eisenstein, so we have that  $2^{1/6}$ , and therefore  $2^{5/6}$ , has degree 6 over  $\mathbb{Q}$ .  $\square$

6. Let  $L/\mathbb{Q}$  denote a Galois extension with Galois group isomorphic to  $A_4$ .

(a) Does there exist a quadratic extension  $K/\mathbb{Q}$  contained in  $L$ ?

*Solution.* By the fundamental theorem of Galois theory, a quadratic extension  $K/\mathbb{Q}$  corresponds to a subgroup of  $\text{Gal}(L/\mathbb{Q}) \cong A_4$  of index 2 (order 6). We claim that there is no such subgroup, and therefore no such quadratic sub-extension.

Any group of order 6 is isomorphic to either  $\mathbb{Z}/6\mathbb{Z}$  or  $S_3$ .  $A_4$  consists of double 2-cycles, e.g.  $(1\ 2)(3\ 4)$ , and 3-cycles, e.g.  $(1\ 2\ 3)$ , none of which have order 6, so that leaves  $S_3$ .  $S_3$  has three elements of order 2, and since the three double 2-cycles in  $A_4$  are exactly its elements of order 2, they must all lie in any subgroup isomorphic to  $S_3$ . However, the elements of order 2 don't commute with one another in  $S_3$  while they do in  $A_4$ , so we cannot have a subgroup of  $A_4$  isomorphic to  $S_3$ .  $\square$

(b) Does there exist a degree 4 polynomial in  $\mathbb{Q}[x]$  with splitting field equal to  $L$ ?

*Solution.*  $\square$

7. Let  $A : V \rightarrow V$  be a linear transformation of a vector space  $V$  over the field  $\mathbb{Q}$  which satisfies the relation  $(A^3 + 3I)(A^3 - 2I) = 0$ . Show that the dimension  $\dim_{\mathbb{Q}}(V)$  is divisible by 3.

*Proof.* Since  $A$  satisfies the polynomial  $(x^3 + 3)(x^3 - 2)$ , the minimal polynomial of  $A$  over  $\mathbb{Q}$  must divide  $(x^3 + 3)(x^3 - 2)$ . Since  $x^3 + 3$  and  $x^3 - 2$  are both irreducible over  $\mathbb{Q}$  by Eisenstein, the minimal polynomial must be either  $x^3 + 3$ ,  $x^3 - 2$  or  $(x^3 + 3)(x^3 - 2)$ . Furthermore, the minimal polynomial divides the characteristic polynomial whose degree is the dimension of  $V$  over  $\mathbb{Q}$ . Since the minimal polynomial and characteristic polynomial have the same roots in an algebraic closure, we must have that the characteristic polynomial is of the form  $(x^3 + 3)^a(x^3 - 2)^b$  for some nonnegative integers  $a, b$  at least one of which is positive. Since the degree of such a polynomial is divisible by 3, we must have that the dimension of  $V$  over  $\mathbb{Q}$  is divisible by 3.  $\square$

8. True/False.

(a) If  $K_1, K_2$  are fields and  $\varphi : K_1 \rightarrow K_2$  is a ring homomorphism such that  $\varphi(1) = 1$ , then  $\varphi$  is injective.

*Solution.* True. The kernel of  $\varphi$  is an ideal in  $K_1$ . Since  $K_1$  is a field its only ideals are  $(0)$  and all of  $K_1$ . Since  $\varphi(1) = 1$ , we have that the kernel of  $\varphi$  is not all of  $K_1$ , so it must be trivial, forcing  $\varphi$  to be injective.  $\square$

(b) The unit group of  $\mathbb{C}$  is isomorphic to the additive group of  $\mathbb{C}$ .

*Solution.* Assuming “the unit group of  $\mathbb{C}$ ” means the nonzero complex numbers,  $\mathbb{C}^\times$ , then this is false.  $\mathbb{C}^\times$  contains an element of order 2,  $-1$ , whereas the additive group  $(\mathbb{C}, +)$  contains no elements of order 2.  $\square$

(c) Let  $n$  be a positive integer. Then  $\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} = 0$ .

*Solution.* True. For any simple tensor  $a \otimes \frac{p}{q}$  in  $\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}$  we have

$$\begin{aligned} a \otimes \frac{p}{q} &= a \otimes \frac{np}{nq} \\ &= na \otimes \frac{p}{nq} \\ &= 0 \otimes \frac{p}{nq} \\ &= 0. \end{aligned}$$

□

9. For each of the following either give an example or show that none exists.

(a) An element  $\alpha \in \mathbb{Q}(\sqrt{2}, i)$  such that  $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, i)$ .

*Solution.* As this is a finite extension of  $\mathbb{Q}$  and since any such extension is separable as  $\mathbb{Q}$  is perfect, the primitive element theorem guarantees the existence of such an  $\alpha$ . We claim that  $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2} + i)$ . The inclusion  $\mathbb{Q}(\sqrt{2} + i) \subseteq \mathbb{Q}(\sqrt{2}, i)$  is obvious. Note that  $(\sqrt{2} + i)^3 = -\sqrt{2} + 5i$ . This gives

$$(\sqrt{2} + i)^3 + (\sqrt{2} + i) = 6i,$$

so  $i \in \mathbb{Q}(\sqrt{2} + i)$ . Subtracting  $i$  from  $\sqrt{2} + i$  shows that  $\sqrt{2} \in \mathbb{Q}(\sqrt{2} + i)$  as well and we have the reverse inclusion. □

(b) A tower of field extensions  $L \supseteq K' \supseteq K$  such that  $L/K'$  and  $K'/K$  are Galois extensions but  $L/K$  is not Galois.

*Solution.* Consider the extensions  $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$  and  $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ . Both of these extensions are Galois since they are quadratic. However,  $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$  is not Galois because it doesn't contain the non-real roots of  $x^4 - 2$ . □

10. Let  $L_1, \dots, L_r$  be all pairwise non-isomorphic complex irreducible representations of a group  $G$  of order 12. What are the possible values for their dimensions  $n_i = \dim_{\mathbb{C}} L_i$ ? For each of the possible answers of the form  $(n_1, \dots, n_r)$  give an example of  $G$  which has such irreducible representations.

*Solution.* We have that  $n_1^2 + \dots + n_r^2 = 12$  and that  $r$  is the number of conjugacy classes in  $G$ . Since the one-dimensional trivial representation is always a representation of  $G$ , we know that at least one of the  $n_i$  is 1. We also know that the number of conjugacy classes divides the order of  $G$  by Lagrange's theorem. These constraints give us three possible configurations of the  $n_i$ :

$$(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \quad (1, 1, 1, 1, 2, 2) \quad (1, 1, 1, 3).$$

Here are some examples from each class.

- (1, ..., 1): The irreducible representations of an abelian group are all one-dimensional, so a group like  $\mathbb{Z}/12\mathbb{Z}$  would fall into this category.
- (1, 1, 1, 1, 2, 2): We can safely place the dihedral group  $D_{12}$  in this category because it has six conjugacy classes and this is the only configuration of the  $n_i$  consistent with this.
- (1, 1, 1, 3): The alternating group  $A_4$  is in this category because it has four conjugacy classes.

□

## Fall 2015

1. (a) Define **prime ideal**.

*Solution.* An ideal  $P \neq R$  of the commutative ring  $R$  is prime if  $ab \in P$  implies that  $a \in P$  or  $b \in P$ . Equivalently,  $P$  is prime if and only if  $R/P$  is an integral domain. □

- (b) Define **maximal ideal**.

*Solution.* An ideal  $I \neq R$  of the ring  $R$  is maximal if  $I$  is not properly contained in another ideal (that isn't all of  $R$ ). If  $R$  is commutative, then  $I$  is maximal if and only if  $R/I$  is a field. □

- (c) Give an example of a ring  $R$  and ideal  $P_1$ ,  $P_2$ , and  $P_3$  of  $R$  such that for the properties “prime ideal” and “maximal ideal” of  $R$ ,
- $P_1$  satisfies both properties,
  - $P_2$  satisfies neither property
  - $P_3$  satisfies one property but not the other.

*Solution.* Let  $R = \mathbb{Q}[x, y]$ . The ideal  $P_1 = (x, y)$  is maximal since  $R/P_1 = \mathbb{Q}$ , which is a field. Since all fields are integral domains, we have that  $P_1$  is prime as well.

The ideal  $P_2 = (x^2)$  is not prime since  $x \cdot x$  is in  $P_2$  but  $x$  is not. Since maximal ideals are always prime, this shows that  $P_2$  isn't maximal either.

The ideal  $P_3 = (x)$  is prime but not maximal since  $R/P_3 = \mathbb{Q}[y]$ , which is an integral domain but not a field. □

2. Show that if a group  $G$  has only finitely many subgroups then  $G$  is a finite group.

*Proof.* Suppose  $G$  is an infinite group. If  $G$  has an element  $g$  of infinite order then  $\langle g \rangle \cong \mathbb{Z}$ , which has infinitely many subgroups. Suppose then that every element of  $G$  has finite order. Since  $G = \cup_{g \in G} \langle g \rangle$  and every  $\langle g \rangle$  is a finite set, the only way to cover the infinite set  $G$  by finite sets  $\langle g \rangle$  is to have infinitely many distinct  $\langle g \rangle$ . Thus, an infinite group must have infinitely many subgroups, so a group with finitely many subgroups must be finite.  $\square$

3. Let  $A$  be an  $n \times n$  matrix with entries in  $\mathbb{R}$  such that  $A^2 = -I$ .

(a) Prove that  $n$  is even.

*Solution.* Since  $A$  satisfies the polynomial  $x^2 + 1$ , its minimal polynomial over  $\mathbb{R}$  must divide  $x^2 + 1$ . This polynomial is irreducible over  $\mathbb{R}$  and since the minimal polynomial divides the characteristic polynomial and both polynomials have the same roots in  $\mathbb{C}$ , the characteristic polynomial must be  $(x^2 + 1)^d$  for some  $d \geq 1$ . The degree of the characteristic polynomial,  $2d$ , is  $n$ , so  $n$  is even.  $\square$

(b) Prove that  $A$  is diagonalizable over  $\mathbb{C}$  and describe the corresponding diagonal matrices.