# August 2000
# Algebra Qualifying Exam
# Sample Solutions

1A) **Answer:** Assume that $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ and $B = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$ then $AB = \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix}$ amd $BA = \begin{bmatrix} ea+fc & eb+fd \\ ga+ch & gb+dh \end{bmatrix}$. Then we compute $\det(AB-\lambda I)$ and $\det(BA-\lambda I)$.

$$\begin{aligned} & \begin{vmatrix} (ea+fc)-\lambda & eb+fd \\ ga+ch & (gb+dh)-\lambda \end{vmatrix} \\ = \; & eagb+eadh+fcgb+fcdh-(ea+fc+gb+dh)\lambda \\ & -(ebga+ebch+fdga+fdch)+\lambda^2 \\ = \; & \lambda^2-(ea+fc+gb+dh)\lambda+eadh+fcgb-ebch-fdga \end{aligned}$$

and

$$\begin{aligned} & \begin{vmatrix} (ae+bg)-\lambda & af+bh \\ ce+dg & (cf+dh)-\lambda \end{vmatrix} \\ = \; & aecf+aedh+bgcf+bgdh-(ae+bg+cf+dh)\lambda \\ & -(ceaf+cebh+dgaf+dgbh) \\ = \; & \lambda^2-(ea+fc+gb+dh)\lambda+eadh+fcgb-ebch-fdga \end{aligned}$$

(b) We use the hint that either $A$ or $B$ is invertible. Assume that $A$ is invertible. Then $A^{-1}(AB)A = BA$ and so $AB$ and $BA$ are similar matrices. Thus we can use the fact that similar matrices have the same characteristic polynomial. Of course we prove the statement. Suppose $Q$ and $R$ are similar matrices. Then there exists invertible $P$ such that $P^{-1}QP = R$. Calculating the characteristic polynomial we have

$$\begin{aligned} \det\left(P^{-1}QP-\lambda I\right) &= \det\left(P^{-1}QP-P^{-1}\lambda IP\right) = \det\left(P^{-1}(Q-\lambda I)P\right) \\ &= \det\left(P^{-1}\right)\det(Q-\lambda I)\det(P) \\ &= \det(P)^{-1}\det(P)\det(Q-\lambda I) = \det(Q-\lambda I) \end{aligned}$$

1B) **Answer:** Let

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

and

$$\det(M-I\lambda) = \lambda^2-(a+d)\lambda+(ad-bc)$$

This has distinct real roots if $(-(a+d))^2-4(ad-bc)^2 > 0$

$$\begin{aligned} & (-(a+d))^2-4(ad-bc) \\ = \; & (a-d)^2+4bc \end{aligned}$$

As $(a-d) \geq 0$ and $bc > 0$ we have distinct real roots, and therefore two distinct eigenvalues, and thus two distinct eigenvectors. Therefore the matrix is diagonalizable.

2A) Determine all finite groups $G$ having a proper subgroup $H$ that contains all proper subgroups of $G$.
**Answer:** cyclic $p$-groups. I will give a long answer as it has lots of nice little claims.
Claim 1: $G$ is a $p$-group.
To see this, note that if $H$ is a subgroup that contains all proper subgroups of $G$, it must contain all Sylow subgroups of $G$. Thus, if it is not a $p$-group, it will be divisible by all prime powers that divide $G$ and consequently will have the same order as $G$ contradicting the fact that it is a proper subgroup.
Claim 2: Any $p$-group has a nontrivial center $Z(G)$.
Use the class equation that $|G| = |Z(G)| + \sum |cl(x)|$

Claim 3: For any $p$-group $G$ with $|G| = p^n$, there exists a subgroup of order $p^k$ for any $k < n$. We prove this by induction. Clearly this is true for $n = 1$. Now assume $|G| = p^{n+1}$. We know $G$ has a nontrivial center by claim 2. In particular, as all subgroups of the center are normal, Cauchy's theorem will guarantee that there is a normal subgroup of size $p$, call it $P$. Then $G/P$ is a group of order $p$ so we can apply the induction hypothesis. Then we use the correspondence theorem to find subgroups in $G$ of order $p^k$ for each $k < n+1$.
Claim 4: If $G$ is a group and $Z(G)$ is the center of $G$ with $G/Z(G)$ cyclic, then $G$ is abelian.

Since $G/Z(G)$ is cyclic, we can find a representative $g$ for the group $G/Z(G)$ which generates $G/Z(G)$. Then any $x \in G$ can be written in the form $g^n z$ for some $z \in Z(G)$ and $g$ the representative we choose. Suppose $x, y \in G$. Then $x = g^n z$ and $y = g^m z'$. So

$$xy = g^n z g^m z' = z z' g^n g^m = z z' g^{n+m} = z z' g^{m+n} = z z' g^m g^n = g^m z' g^n z = yx.$$

And therefore $G$ is abelian. Note: That if $H \leq Z(G)$, then we can make the same argument for $G/H$.
Claim 5: If $G$ is a $p$-group and has a unique subgroup of index $p$ then it is cyclic.
We prove this by induction. For $n = 1$ it is trivial. Assume $|G| = p^{n+1}$. Now let $P$ be a subgroup of the center of order $p$. Then we have that $G/P$ has order $p^n$. Now it must have a subgroup of index $p$ by claim 3. Moreover, by the correspondence theorem it must be unique. Thus by the induction hypothesis, it must be cyclic. But following the note after claim 4, $G$ must be abelian. Now using the fundamental theorem for finite abelian groups, we have $G \cong \mathbb{Z}_{p^n} \oplus \mathbb{Z}_p$ or $G \cong \mathbb{Z}_{p^{n+1}}$, i.e. $G$ is cyclic.

Now we finally prove the answer. We know that $G$ is a $p$-group by claim 1. By claim 3, there exists subgroups of order $p^k$ for every $k < n$, so if $G$ has a subgroup which contains all other subgroups, it must have maximal order, i.e. it must have index $p$ in $G$. Also, since it contains all subgroups, it must be the unique subgroup of index $p$. Thus by claim 5, it must be cyclic. So we know the structure it must have, and it is not hard to see that there are sufficient conditions also, i.e. any cyclic group of order $p^n$ has a subgroup which contains all other subgroups (namely the subgroup generated by $x^p$ where $x$ generates $G$).

2B) Let $G$ be a finite group with exactly two conjugacy classes of elements. Determine the possible isomorphism types for $G$.
**Answer:** We know that the identity is always its own conjugacy class. Therefore there is only one other conjugacy class. We also know that for each $x \in Z(G)$, $x$ is its own conjugacy class. Some other claims we use.
Claim 1: Conjugacy class preserves the order of an element.
Let $g \in G$ and suppose it has order $n$. Then for any $x \in G$ with order $n$,

$$\left(xgx^{-1}\right)^n = xgx^{-1}xgx^{-1}\cdots xgx^{-1} = xg^n x^{-1} = 1.$$

Thus $n$ divides the order of $xgx^{-1}$ which say is $d$. Then we know that if $xgx^{-1}$ has order $d$ then

$$\left(xgx^{-1}\right)^d = xg^d x^{-1} = 1$$

and this implies that $g^d = 1$ and so $d|n$. Thus $d = n$ and they have the same order.
Claim 2: $G$ must have order $p$ for $p$ a prime.
The identity element is one conjugacy class. All others fall into the same class and so must have the same order. Clearly they must have order a prime else Cauchy's theorem would guarantee elements of order $n$ where $n$ divides $p$ thus giving different conjugacy classes.
Now note that any group of order $p$ where $p$ is a prime is cyclic. In particular, it will be abelian and thus every conjugacy class will have size one. In particular the number of conjugacy classes $= |G| = p$, and since there are only two by assumption, this is only true for $p = 2$. Thus $\mathbb{Z}_2$ is the only group with this property.

3A) Determine (up to isomorphism) all semisimple rings having 324 elements.
**Answer:** By the Wedderburn-Artin theory if we have a semisimple Artinian ring (which is true as the ring is finite), then we know that the ring is the direct sum of full matrix algebras over a division ring (which is a field because a finite division ring is a field, another theorem of Weddeburn). Therefore the possibilities are

$\mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_3 \times \mathbb{F}_3 \times \mathbb{F}_3 \times \mathbb{F}_3$, $\mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_{3^2} \times \mathbb{F}_3 \times \mathbb{F}_3$, $\mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_{3^2} \times \mathbb{F}_{3^2}$, $\mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_{3^3} \times \mathbb{F}_3$, $\mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_{3^4}$, $\mathbb{F}_{2^2} \times \mathbb{F}_3 \times \mathbb{F}_3 \times \mathbb{F}_3 \times \mathbb{F}_3$, $\mathbb{F}_{2^2} \times \mathbb{F}_{3^2} \times \mathbb{F}_3 \times \mathbb{F}_3$, $\mathbb{F}_{2^2} \times \mathbb{F}_{3^2} \times \mathbb{F}_{3^2}$, $\mathbb{F}_{2^2} \times \mathbb{F}_{3^3} \times \mathbb{F}_3$, $\mathbb{F}_{2^2} \times \mathbb{F}_{3^4}$, $\mathbb{F}_2 \times \mathbb{F}_2 \times M_2(\mathbb{F}_3)$, $\mathbb{F}_4 \times M_2(\mathbb{F}_3)$.

3B) (a) Let $R$ be a finite integral domain. Show $R$ is a field.

(b) Let $R$ be a commutative ring with identity and let $I$ be a prime ideal of finite index in $R$. Show that $I$ is a maximal ideal.
**Answer:** (a) For each $r \in R$ we can define a map $\Psi_a : R \to R$ by left multiplication of $a$ for each $a \in R^*$. This will be a 1-1 map since $R$ is a domain. It must be onto since we have a 1-1 map from a finite set to a finite set.Thus there exists $x \in R$ such that $ax = 1$, i.e. each $a$ is a unit. Or we can use that fact that if we have an $a \in R^*$ then we have $a, a^2, ..., a^n, ..., a^r$ and since our ring is finite we must have $a^n = a^r$ for some $r > n$. Thus $a^{n-r}a^n = a^n$ and $a^{n-r}$ is the identity for $a^n$. This identity must be the identity for the entire ring by the following:
To prove there is an identity, we may assume there is an $e_a$ and $e_b$ such that $e_a a = a$ and $e_b b = b$. If $e_a \neq e_b$ then $e_a - e_b \neq 0$. As $a, b \neq 0$ we know that $ab \neq 0$ and so $ab(e_a - e_b) \neq 0$. This is a contradiction as using commutativity we have $ab(e_a - e_b) = ab - ab = 0$
(b) Claim: $R/I$ is an integral domain.
Assume that $(x + I)(y + I) = I$. This implies that $xy + I = I$ implies $xy \in I$. As $I$ is a prime ideal we have that $x \in I$ or $y \in I$. Thus $x + I = I$ or $y + I = I$ and so $R/I$ is an integral domain.
It is a finite integral domain and therefore a field. Therefore as $R/I$ is a field, we have that $R/I$ is simple and thus $I$ is a maximal ideal.

4A) Let $K = \mathbb{F}_{81}$, the field with 81 elements, with prime field $\mathbb{F}_3$. Determine, with reasons, the cardinalities of the following two subsets of $K$.
(a) $S = \{s \in K : F(a) = K\}$, generators for $K$ as a field extension of $F$.
(b) $T = \{a \in K : \langle a \rangle = K^* = K \setminus \{0\}\}$, generators for the (multiplicative) cyclic group $K^*$.
**Answer:** (a) As $\mathbb{F}_{81}$ is a degree four extension of $\mathbb{F}_3$ it has $\mathbb{F}_9$ as its only intermediary subfields. Therefore if we take $s \in \mathbb{F}_{81} \setminus \mathbb{F}_9$ then we know that if we adjoin one of these that we will have generated the whole field $\mathbb{F}_{81}$. Therefore the answer is 72.
(b) One way to think of this problem is that $|T|$ is the same as the number of generators of the cyclic group $\mathbb{Z}_{80}$. This is just $\varphi(80)$, the Euler phi operatornametion. The total is 32. Note: $\varphi(80) = \varphi\left(2^4\right)\varphi(5)$ and $\varphi(p^n) = (p-1)p^{n-1}$ and so we have $(2-1)2^3 \cdot (5-1)5^0 = 32$.

4B) Determine the Galois group over $\mathbb{Q}$ of $f(x) = x^3 - 3x + 1$.
**Answer:** The first thing we note is that $f(x)$ is irreducible. We see this by reduction mod 2. We get $f(x) = x^3 + x + 1$ and $f(0) = 1$ and $f(1) = 1$. By simple calculus we can show that this operatornametion has three real roots. As the polynomial is irreducible, we know that the Galois group is a transitive subgroup of $S_3$. Therefore it is either $A_3$ or $S_3$. But we have no element of order two and therefore it is $A_3$. The other way to do this is to note that it is already in the nice form to compute a discriminant. The discriminant is 81 which has a root in 9 which means that it is $A_3$.

5A) Show that $\mathbb{Q}$ is not a free $\mathbb{Z}$-module.
**Answer:** Assume that $\mathbb{Q}$ is a free $\mathbb{Z}$-module. Then there is a basis $\{b_i\}_{i \in \mathcal{I}}$ such that all $q \in \mathbb{Q}$ can be written as a finite sum $q = \sum a_i b_i$ for $a_i \in \mathbb{Z}$. If the basis has size one then we could choose $\frac{s}{t}$ as the basis element for $(s, t) = 1$ and $s, t \neq 0$. Let $t = p_1^{k_1} \cdots p_n^{k_n}$ be the prime factorizati0n of $t$. Pick another prime $q \in \mathbb{Q}$ not in the factorization of $t$. Then we can show that $\frac{1}{q}$ cannot be expressed as a $\mathbb{Z}$-scalar multiple of $\frac{s}{t}$. Therefore the basis has cardinality greater than 1. So take two basis elements $\frac{s}{t}$ and $\frac{u}{v}$. Then we have that

$$(tu)\left(\frac{s}{t}\right) + (-vs)\left(\frac{u}{v}\right) = us - us = 0$$

and therefore any basis of size greater than 1 is linearly dependent.

5B) Describe the abelian group with the presentation

$$A = \langle a, b, c : 4a + 10b - 8c = 0, 2a + 8b - 4c = 0 \rangle$$

as a direct sum of cyclic groups.

**Answer:** We use the procedure of finding smith normal form.

$$\begin{pmatrix} 4 & 10 & -8 \\ 2 & 8 & -4 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & 8 & -4 \\ 4 & 10 & -8 \end{pmatrix}$$
$$\longrightarrow \begin{pmatrix} 2 & 8 & -4 \\ 0 & -6 & 0 \end{pmatrix}$$
$$\longrightarrow \begin{pmatrix} 2 & 0 & 0 \\ 0 & -6 & 0 \end{pmatrix}$$

Therefore the group is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}$ as there is one free generator.