Algebra Comprehensive Exam
— Fall 2008 —

Instructions: Complete five of the seven problems below. If you attempt more/less than five questions, then **circle** in the box below

1	2	3	4	5	6	7

which five should be graded. Uncircled problems will *not* be graded.

(1) (a) If G is a finite group with 125 elements, prove that its center Z is non-trivial.
(b) Prove that there is no finite group G with 125 elements whose center Z has 25 elements.
(c) Construct a non-abelian group G with 125 elements and with center Z a cyclic group of order 5.

Solution. (a) Let G act on $X = G$ by conjugation. The size of the conjugacy class of $g \in G$ is $|G|/|C(g)|$ where $C(g)$ is the centralizer of g in G. Thus, the size of the conjugacy class is 5^k for $k = 1, 2, 3$. $k = 1$ iff $g \in Z$ and $|Z|$ divides 125. Since $125 = |X|$ and 5 divides the size of every non-trivial conjugacy class, it follows that 5 divides $|Z|$.

(b) If $|G| = 125$ and $|Z| = 25$, take $g \in G \setminus Z$ and consider the centralizer $C(g)$. $|C(g)|$ divides 125 and $C(g)$ contains Z and g, so $C(g)$ strictly contains Z. So $C(g) = G$ which implies that $g \in Z$ a contradiction.

(c) Let G denote the set of upper-triangular matrices with 1 on the diagonal and entries in $\mathbb{Z}/3$. G is a group under multiplication. Indeed if $A \in G$ then $A = I - N$ where N is stricly upper triangular; thus $N^3 = 0$. So $A^{-1} = I + N + N^2$ is in G. Likewise, G is closed under multiplication. Indeed if $A = I + N_1$, $B = I + N_2$, then $AB = I + (N_1 + N_2 + N_1 N_2)$. So G is a group of order 125. If A, B are general elements of G with 12 and 23 entries a, c and x, z respectively then $AB - BA$ has 13 entry $-cx + az$ and all others zero. It follows that Z consists of all matrices with 13 entry arbitrary and all other entries zero. Z is indeed a group of order 5. $\square$

(2) Let S_4 denote the group of permutations of $\{1, 2, 3, 4\}$.
(a) How many elements are in the conjugacy class C of $(12)(34)$?
(b) How many 2-Sylow subgroups does S_4 have?
(c) List all permutations in your favorite 2-Sylow subgroup of S_4.

Solution. (a) Two permutations in S_n are conjugate iff they have the same cycle type, corresponding to a partition λ of n, where λ contains n_1 cycles of type 1, n_2 cycles of type 2 etc, where $n = \sum_k k n_k$. Then C contains $n!/\prod_k k^{n_k} n_k!$ elements. In our case $n_2 = 2$ and $n_k = 0$ for $k \neq 2$. Thus there are 3 elements in the conjugacy class 2^2.

(b) $|S_4| = 4! = 24$. If P is a 2-Sylow subgroup, then $|P| = 8$. The number of 2-Sylow subgroups is $1 + 2k$ which divides 24. So there is either 1 or 3 2-Sylow subgroups. If there is only one such, then P is normal of order 8. The conjugacy class of type $1^2 2$ has 6 elements, the one of type 1^4 has 1 element, the one of type 4 has 6 elements. Since P contains an element of oder 2, it follows that it contains elements of the conjucacy class 2^2, $1^2 2$ or 4. The square of an element of type 4 is an element of type 2^2. In all cases, $P - 1$, a set with 7 elements is a union of conjugacy classes and the above numbers do not work giving a contradiction. So there are 3 2-Sylow subgroups in S_4.

(c) By trial, the following set P is a group of order 8:

$$\{1, (12), (34), (12)(34), (13)(24), (14)(23), (1324), (1423)\}$$

□

(3) Let A_n denote the alternating group of n elements.
  (a) Can A_4 be mapped homomorphically onto $\mathbb{Z}/2$?
  (b) Can A_5 be mapped homomorphically onto $\mathbb{Z}/2$? Reason your answers.

Solution. (b) A_5 is simple; the kernel of a nontrivial homomorphism into a group is normal, so the answer is no for A_5.

(a) If $\phi : A_4 \to \mathbb{Z}/2$ is onto, the kernel K has order 6. A_4 has four conjugacy classes 1, (123), (132) and (12)(34) with 1, 4,4 and 3 elements (compare with Fulton-Harris: Representation Theory, exercise 2.26). Since K is a union of conjugacy classes, this is not possible. No such homomorphism exists. □

(4) Suppose that $R \subseteq \mathbb{C}$ is a ring that also is a finitely generated free $\mathbb{Z}$-module. Let $\alpha \in \mathbb{C}$ have the property that $\alpha R \subseteq R$. Show that α is a root of a monic, irreducible polynomial in $\mathbb{Z}[x]$.
Hint: Think of multiplication of R by α as acting like a linear transformation.

Solution. Let $x_1, ..., x_k$ be a $\mathbb{Z}$ basis of R. The fact that $\alpha R \subseteq R$ implies that $\alpha x_i \in R$ for $i = 1, ..., k$. From the fact that R is a free module with basis $x_1, ..., x_k$ we deduce that

$$\begin{aligned} \alpha x_1 &= a_{1,1}x_1 + \cdots + a_{1,k}x_k \\ \alpha x_2 &= a_{2,1}x_1 + \cdots + a_{2,k}x_k \\ &\vdots \\ \alpha x_k &= a_{k,1}x_1 + \cdots + a_{k,k}x_k. \end{aligned}$$

Letting M denote the $k \times k$ matrix of the $a_{i,j}$, we find that we may rewrite this in matrix notation as

$$\alpha \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{bmatrix} = M \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{bmatrix}.$$

So, α is an eigenvalue of the integer matrix M, and it follows therefore that α is a root of

$$\det(M - xI).$$

Upon multiplying through by -1 if needed, we see that this polynomial is monic in $\mathbb{Z}[x]$, and therefore so is the minimal polynomial of α. □

(5) Fix a prime number p, and let α lie in an extension field of $\mathbb{F}_p$ of degree r, and let β lie in an extension field of $\mathbb{F}_p$ of degree s where r and s are distinct prime numbers. Furthermore, assume $\alpha, \beta \notin \mathbb{F}_p$. Prove that $\alpha + \beta$ lies in $\mathbb{F}_{p^{rs}}$ but does not lie in any smaller field.

Solution. Let F denote $\mathbb{F}_p[\alpha]$, G denote $\mathbb{F}_p[\beta]$, H denote $\mathbb{F}_p[\alpha + \beta]$, and K denote $\mathbb{F}_p^{rs}$.
Clearly, we have the chain

$$\mathbb{F}_p \subseteq H \subseteq K.$$

We will now try to show that $[H : \mathbb{F}_p] = rs$: We begin by noting that this degree divides rs, so is either $1, r, s$ or rs, since r and s are distinct primes. It cannot be 1, since it would mean that $\alpha + \beta \in \mathbb{F}_p$, which would therefore mean $\mathbb{F}_p[\alpha] = \mathbb{F}_p[\beta]$.

Suppose the degree is r. Then, since there is only one degree r extension of $\mathbb{F}_p$ (it is the unique field fixed by the rth power of the Frobenius automorphism), we would be forced to conclude

$$F \;=\; H;$$

so, $\alpha + \beta \in F$, which implies $\beta \in F$. So, G is a proper subfield of F, which easily implies $G = \mathbb{F}_p$, contradiction.

We similarly reach a contradiction if we suppose the degree was s. It follows therefore that the degree of H is rs, and we are done. $\square$

(6) Let G be the set $\mathbb{Z}_3 \times \mathbb{Z}_7$, with the following addition operation $\oplus$:

$$(a,b) \oplus (c,d) \;=\; (a+c \pmod 3,\; b \cdot 2^c + d \pmod 7).$$

(a) Show that this makes G into a group.
(b) Show that this group G is non-abelian.
(c) Expalin why the following $*$ is not an operation on $\mathbb{Z}_3 \times \mathbb{Z}_5$:

$$(a,b) * (c,d) \;=\; (a+c \pmod 3,\; b \cdot 2^c + d \pmod 5)).$$

Solution. (a) The identity of this group will be $(0,0)$: We have that

$$(a,b) \oplus (0,0) \;=\; (a,\; b \cdot 2^0 + 0) \;=\; (a,b).$$

Likewise, $(0,0) \oplus (a,b) = (a,b)$.

Let's check associativity:

$$\begin{aligned} ((a,b) \oplus (c,d)) \oplus (e,f) &= (a+b \pmod 3,\; b \cdot 2^c + d \pmod 7)) \oplus (e,f) \\ &= ((a+b)+e \pmod 3,\; (b \cdot 2^c + d)2^e + f \pmod 7)) \\ &= (a+b+c \pmod 3,\; b \cdot 2^{c+e} + d \cdot 2^e + f \pmod 7)). \end{aligned}$$

On the other hand,

$$\begin{aligned} (a,b) \oplus ((c,d) \oplus (e,f)) &= (a,b) \oplus (c+e \pmod 3,\; d \cdot 2^e + f \pmod 7)) \\ &= (a+(c+e) \pmod 3,\; b \cdot 2^{c+e} + d \cdot 2^e + f \pmod 7)). \end{aligned}$$

Clearly, then, we have that associativity holds. Note the following subtle point: When we computed 2^{c+e} in this last line, we note that the value of $c+e$ was only defined modulo 3 – that's ok, though, because 2 is cyclic of order 3 under multiplication modulo 7 (so, there is no issue here with 2^{c+e} being well-defined).

We need to check for inverses: We claim that the inverse of (a,b) is the element $(-a, -b \cdot 2^{-a})$. This is easily seen to hold, as

$$(a,b) \oplus (-a, -b \cdot 2^{-a}) \;=\; (0 \pmod 3,\; b \cdot 2^{-a} - b \cdot 2^{-a} \pmod 7)) \;=\; (0,0).$$

Lastly, we should point out that $\oplus$ is well-defined, and the main reason is that the powers of 2 form a cyclic group of order 3 under multiplication modulo 7 – this is what allows us to write $2^a \pmod 7$, as its value is the same regardless of which element of the residue class $a \pmod 3$ we choose for the exponent of 2.

It is worth pointing out that the group you are being asked to prove is actually a semi-direct product in disguise.

(b) To show G is non-abelian, consider the pair

$$(1,1) \;\oplus\; (0,1) \;=\; (1,\; 2),\ \text{yet}\ (0,1) \;\oplus\; (1,1) \;=\; (1,\; 3).$$

(c) The reason * is not an operation is that it is not well-defined. More specifically, the exponentiation $2^c \pmod 5$ does not make sense. For example, suppose $c \equiv 1 \pmod 3$.

Then, if we were to use $c = 1$ we would have $2^c \equiv 2 \pmod 5$, but if we were to use $c = 6$ we would have $2^6 \equiv 4 \pmod 5$.

$\square$

(7) Let R be a commutative ring, and let I be an ideal of R. We define the "radical of I" to be the set

$$\mathrm{Rad}(I) \ := \ \{x \in R \ : \ \text{there exists } m \geq 1 \text{ such that } x^m \in I\}.$$

(a) Show that $\mathrm{rad}(I)$ is an ideal of R.
(b) Compute the radical of the ideal $I \ := \ 108\mathbb{Z} \subset \mathbb{Z}$.

Solution. (a) Suppose that $\alpha, \beta \in \mathrm{Rad}(I)$. Then, there exists $r, s \geq 1$ such that $\alpha^r, \beta^s \in I$. By closure properties of I we have that upon letting $m = \max(r, s)$, $\alpha^m, \beta^m \in I$. To show that $\alpha + \beta \in \mathrm{Rad}(I)$, observe that by the binomial theorem for commutative rings,

$$(\alpha + \beta)^{2m} \ = \ \sum_{j=0}^{2m} \binom{2m}{j} \alpha^j \beta^{2m-j}.$$

Every single term of this sum involves either a power of α that is $\geq m$, or a power of β that is $\geq m$. So, in each term, one of the factors belongs to I, which therefore means the term itself belongs to I (by the multiplicative property of ideals), and therefore the whole sum belongs to I, by the sum-closure property of ideals. We have thus shown $(\alpha + \beta)^{2m} \in I$, whence $\alpha + \beta$ is in $\mathrm{Rad}(I)$.

Lastly, suppose $t \in R$ and $\alpha \in \mathrm{Rad}(I)$. Since $\alpha^r \in I$ for some r, by multiplicative property of ideals we have $(t\alpha)^r = t^r \alpha^r \in I$, whence $t\alpha \in \mathrm{Rad}(I)$. This completes the proof that the radical is an ideal.

(b) We factor $108 = 2^2 3^3$. It is clear that the radical of $108\mathbb{Z}$ contains $6\mathbb{Z}$. Furthermore, every element of the radical must be divisible by 2 and 3, so equals $6\mathbb{Z}$.

In general, for $d \geq 1$, the radical of the ideal $d\mathbb{Z}$ is $d'\mathbb{Z}$, where d' is the product of all the distinct primes dividing d. $\square$