Math 318 Final Exam; Solutions May 12, 2004

1. If $K$ is a finite field, prove that there is a prime $p$ and an integer $n \geq 1$ with $|K| = p^n$.

If $k$ is the prime field of $K$, then $k \cong \mathbb{F}_p$ for some prime $p$ (the only other possibility is that $k \cong \mathbb{Q}$, which is impossible here because $\mathbb{Q}$ is infinite). But $K$ is a vector space over $k$ (elements $\alpha \in K$ are the vectors and elements $a \in k$ are the scalars, with scalar multiplication $a\alpha$ being the given product of two elements in $K$). Since $K$ is finite, a basis of $K$ over $k$ must be finite, so that $\dim_k (K) = n$ for some $n \geq 1$. Hence, $K \cong k^n$, and so $|K| = |k^n| = p^n$.

2. Let $A$ be an $n \times n$ matrix over a field $k$. Recall that $c$ is an eigenvalue of $A$ if $h(c) = 0$, where $h(x) \in k[x]$ is the characteristic polynomial of $A$.

(i). (15 points) Prove that there is a field $K$ containing $k$ as subfield so that $c$ is an eigenvalue of $A$ if and only if there is a nonzero vector $v \in K^n$ with $Av = cv$.

By Kronecker’s theorem, there is a field $K$ containing $k$ as a subfield and which contains all the roots of $h(x)$, the characteristic polynomial of $A$.

If $Av = cv$, where $v \neq 0$, then the homogeneous system $(cI - A)x = 0$ has a nontrivial solution; hence, $\det(cI - A) = 0$. Therefore, $c$ is a root of $\det(xI - A) = h(x)$; that is, $c$ is an eigenvalue of $A$.

Conversely, consider the $n \times n$ system of linear equations $(cI - A)x = 0$. This is a system over the field $K$ (for $c$ may not lie in $k$). By hypothesis, $\det(cI - A) = 0$, and so there is a nontrivial solution $v \in K^n$; that is, $v \neq 0$, $(cI - A)v = 0$, and $Av = cv$.

(ii). (10 points) Prove that $A^m = 0$ for some $m \geq 1$ if and only if every eigenvalue of $A$ is 0.

If $c$ is an eigenvalue of $A$, then there is a nonzero vector $v \in K^n$ with $Av = cv$. We know (or can prove by induction on $m \geq 1$) that $A^m v = c^m v$. Hence, if $A^m = 0$, then $c^m v = 0$. Since $v \neq 0$, we have $c^m = 0$, and so $c = 0$.

Conversely, if every eigenvalue of $A$ is 0, then the characteristic polynomial $h(x)$ of $A$ is $x^n$ (because $h(x) = \prod_{i=1}^n (x - c_i)$, where $c_i$ are the eigenvalues of $A$). It now follows from the Cayley-Hamilton theorem (which says that $h(A) = 0$) that $A^n = 0$.

3. Let $A$ and $B$ be $n \times n$ matrices over a field $k$. If $AB = I$, prove that $BA = I$.

Let $E$ be the standard basis of $k^n$, let $S: k^n \rightarrow k^n$ be the linear transformation defined by $S(v) = Av$, and let $T: k^n \rightarrow k^n$ be the linear transformation defined by $T(v) = Bv$. In the notation of the course,

$$A = E[S]_E \quad \text{and} \quad B = E[T]_E.$$
We know that
\[ AB = (E[S]E)(E[T]E) = E[S \circ T]E, \]
so that \( E[S \circ T]E = I \). Therefore, \( S \circ T = 1_{k^n} \), so that it is a result of set theory that \( S \) is surjective and \( T \) is injective. It follows that \( \text{im} \, T \cong k^n \), so that \( \dim(T) = n \). But if \( W \subseteq V \) and both vector spaces have the same finite dimension \( n \), then \( W = V \). Therefore, \( T \) is surjective, and hence \( T \) is an isomorphism. Finally, \( S \circ T \circ T^{-1} = T^{-1} \), and so \( S \) and \( T \) commute. That is, \( T \circ S = 1 \).

4 (i). (15 points) To similarity, find all \( 2 \times 2 \) real matrices \( A \) such that \( A^2 = I \).

Since \( A \) satisfies \( A^2 = I \), its eigenvalues are \( \pm 1 \). These eigenvalues are real, and so we may use the Jordan canonical form. The \( 1 \times 1 \) Jordan blocks are \( \begin{bmatrix} 1 \end{bmatrix} \) and \( \begin{bmatrix} -1 \end{bmatrix} \), while the \( 2 \times 2 \) Jordan blocks are \( \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \) and \( \begin{bmatrix} -1 & 0 \\ 1 & -1 \end{bmatrix} \).

There are 5 similarity classes. Besides the \( 2 \times 2 \) Jordan blocks, there are \( \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \), \( \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \), and \( \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \).

Note that \( \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \) and \( \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \) are similar, because permuting the Jordan blocks does not change the similarity class.

(ii). (10 points) Let \( G \) be the additive group of all \( 2 \times 2 \) matrices over a field \( k \). Prove that trace is a linear transformation \( \text{tr} : G \to k \), and find a basis of \( \ker \text{tr} \).

Since \( \text{tr}(\begin{bmatrix} a & b \\ c & d \end{bmatrix}) = a + d \), it is easy to see that \( \text{tr}(A + B) = \text{tr}(A) + \text{tr}(B) \) and \( \text{tr}(\alpha A) = \alpha \text{tr}(A) \). Now \( \text{tr} : G \to k \) is surjective: if \( \alpha \in k \), then \( \text{tr}(A) = \alpha \), where \( A = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \). Therefore, \( \dim(\text{im} \, \text{tr}) = 1 \). Since \( \dim(G) = 4 \), we have \( \dim(\ker \text{tr}) = 3 \). In more detail, a matrix \( A \in \ker \text{tr} \) if and only if \( A = \begin{bmatrix} a & b \\ c & -a \end{bmatrix} \), and a basis for \( \ker \text{tr} \) is \( \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \).

5. If \( G \) is a group, then its \textit{commutator subgroup} \( G' \) is defined to be the subgroup of \( G \) generated by \( \{xyx^{-1}y^{-1} : x, y \in G\} \). In a previous exam, we proved that \( G' \triangleleft G \) and that \( G/G' \) is abelian.

5 (i). (10 points) If \( H \triangleleft G \) and \( G/H \) is abelian, prove that \( G' \triangleleft H \).

It suffices to show that every generator of \( G' \) lies in \( H \). If \( x, y \in G \), then \( xHyH = yHxH \) in \( G/H \). Therefore, \( xyH = yxH \), and so \( x^{-1}y^{-1}xy \in H \) for
all \( x, y \in G \). In we replace \( x \) by \( x^{-1} \) and \( y \) by \( y^{-1} \), then we have \( xyx^{-1}y^{-1} \in H \), as desired.

(ii). (15 points) If \( S \) is a subgroup of \( G \) and \( G' \leq S \), prove that \( S \triangleleft G \).

Since \( G' \leq S \), we have \( S/G' \leq G/G' \). But \( G/G' \) is abelian, so that every subgroup is normal. In particular, \( S/G' \triangleleft G/G' \), and the correspondence theorem gives \( S \triangleleft G \).

6 (i). (15 points) Find all those permutations in \( S_6 \) that commute with \( \alpha = (1 \ 2 \ 3)(4 \ 5 \ 6) \).

**Hint.** Consider \( \sigma = (1 \ 4 \ 2 \ 5 \ 3 \ 6) \).

We know that two permutations are conjugate in \( S_n \) if and only if they have the same cycle structure. The number of permutations in \( S_6 \) having the same cycle structure as \( \alpha \) is

\[
\frac{1}{2} \left( \frac{6 \cdot 5 \cdot 4}{3} \times \frac{3 \cdot 2 \cdot 1}{3} \right) = 40,
\]

the “extra” factor \( \frac{1}{2} \) occurring so that \((a \ b \ c)(d \ e \ f) = (d \ e \ f)(a \ b \ c)\) not be counted twice.

We use the orbit-stabilizer theorem: \( |\alpha^S_6| = |S_6 : C_{S_6}(\alpha)| \). We have

\[
40 = |\alpha^S_6| = |S_6 : C_{S_6}(\alpha)| = \frac{720}{|C_{S_6}(\alpha)|},
\]

so that

\[
|C_{S_6}(\alpha)| = \frac{720}{40} = 18.
\]

We can exhibit these elements: if \( \beta = (1 \ 2 \ 3) \) and \( \gamma = (4 \ 5 \ 6) \), then \( \beta^i \gamma^j \) commutes with \( \alpha \) for \( 0 \leq i, j \leq 2 \). Thus, we have displayed 9 elements commuting with \( \alpha \). The hint suggests that you try \( \sigma = (1 \ 4 \ 2 \ 5 \ 3 \ 6) \). It turns out that \( \sigma \alpha = \alpha \sigma \), and so \( \sigma \beta^i \gamma^j \) also commutes with \( \alpha \). We have now displayed 18 such elements, and there can be no others. (You may wonder whether these 18 elements form a subgroup, as they must. They do, and the theological reason for this is that \( \sigma^2 = \alpha \).

(ii). (10 points) Find all those permutations in \( A_6 \) that commute with \( \alpha = (1 \ 2 \ 3)(4 \ 5 \ 6) \).

In part (i), we saw that there are 18 permutations in \( S_6 \) commuting with \( \alpha \). But \( \sigma \), being a 6-cycle, is an odd permutation, and so the only even permutations commuting with \( \alpha \) have the form \( \beta^i \gamma^j \).

7. Let \( p \) be an odd prime, and define \( G \) to be the set of all matrices of the form

\[
\begin{bmatrix}
1 & a & b \\
0 & 1 & c \\
0 & 0 & 1
\end{bmatrix},
\]

where \( a, b, c \in I_p \).
(i). (10 points) Prove that $G$ is a group (under matrix multiplication) of order $p^3$.

It suffices to show that $G$ is a subgroup of $\text{GL}(3, \mathbb{F}_p)$. Obviously, $I \in G$.

If \[
\begin{bmatrix}
1 & a & b \\
0 & 1 & c \\
0 & 0 & 1
\end{bmatrix}
\] \in G and \[
\begin{bmatrix}
1 & x & y \\
0 & 1 & z \\
0 & 0 & 1
\end{bmatrix}
\] \in G, then their product is \[
\begin{bmatrix}
1 & a+x & y+az+b \\
0 & 1 & c+z \\
0 & 0 & 1
\end{bmatrix}
\] \in G.

Finally, \[
\begin{bmatrix}
1 & a & b \\
0 & 1 & c \\
0 & 0 & 1
\end{bmatrix}
\] \begin{bmatrix}
1 & a & b \\
0 & 1 & c \\
0 & 0 & 1
\end{bmatrix}^{-1} = \begin{bmatrix}
1 & -a & ac-b \\
0 & 1 & -c \\
0 & 0 & 1
\end{bmatrix} \in G.

(ii). (15 points) Prove that $A^p = I$ for every $A \in G$.

We have $A = I + N$, where $N = \begin{bmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{bmatrix}$. Note that $N^3 = 0$. Since $I$ and $N$ commute, the binomial theorem gives

\[
A^p = (I + N)^p = I^p + N^p + \sum_{i=1}^{p-1} \binom{p}{i} N^i = I + N^p,
\]

because $\binom{p}{i} \equiv 0 \mod p$. Since $p \geq 3$ and $N^3 = 0$, we have $N^p = 0$, and so $A^p = I$.

8 (i). (5 points) Give an example of a finite group $G$ whose center, $Z(G)$, is $\{1\}$.

Let $G = S_3$. We claim that $Z(S_3) = \{1\}$. The only nontrivial subgroups are $S_3$ itself, which is not the center because it is not abelian, or the cyclic subgroups, generated by a 2-cycle or a 3-cycle. But $(1 \ 2)(1 \ 2 \ 3) = (2 \ 3) \neq (1 \ 3) = (1 \ 2 \ 3)(1 \ 2)$. This can be generalized to show that no 2-cycle commutes with a 3-cycle.

8 (ii). (20 points) Prove that the center, $Z(G)$, of a finite $p$-group $G$ has more than one element.

This follows from the class equation:

\[
|G| = |Z(G)| + \sum \left| \frac{G}{C_G(x_i)} \right|,
\]

where one $x_i$ is chosen from each conjugacy class in $G$ having more than one element. Since $G$ is a $p$-group, we have $p \mid |G|$ and $p \mid \left| \frac{G}{C_G(x_i)} \right|$ for all $i$. Therefore, $p \mid |Z(G)|$ and $Z(G) \neq \{1\}$. 