Matrix groups and fields.

1. $GL_2(\mathbf{F}_2)$ consists of the following matrices with entries in $\mathbf{F}_2$:

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad .$$

Consider the following set of matrices in $GL_2(F)$, for (i) $F = \mathbf{R}$ and (ii) $F = \mathbf{F}_{11}$:

$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix} \quad \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \quad \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \begin{bmatrix} b & a \\ a & -b \end{bmatrix} \quad \begin{bmatrix} -b & a \\ a & b \end{bmatrix} \quad \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad ,$$

where (i) $a = -1/2$, $b = \sqrt{3}/2$ in $F = \mathbf{R}$, and (ii) $a = 5$ and $b = 8$ in $F = \mathbf{F}_{11}$.

For any field F, the set of "permutation matrices" in $GL_3(F)$ comprises

$$\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \quad .$$

CHECK: Each of the four sets of matrices is a group. In each of them, one can find elements A and B, such that the other elements are A^2, AB, BA, and I. The "generators" A and B satisfy the conditions:

$$A^3 = I, \quad B^2 = I, \quad BA = A^2B \quad .$$

The next exercise will show that these rules completely determine the multiplication table of each group. Hence the four groups of matrices described above are mutually isomorphic.

2. Let G be a group consisting of exactly six elements e, s, s^2, t, st, s^2t, with e neutral, and satisfying the rules

$$s^3 = e, \quad t^2 = e, \quad ts = s^{-1}t \, .$$

Write out the multiplication table for G.

3. In $GL_2(\mathbf{F}_2)$, the set of matrices $\{0, I, A, A^2\}$ is closed under addition, and forms a field. Let us call it $\mathbf{F}_4$. There are exactly two isomorphism between $\mathbf{F}_4^\times$ and the additive group of $\mathbf{F}_3$.

4. In $GL_2(\mathbf{F}_3)$, find a matrix J such that $J^2 = -I$. The subset $\{aI + bJ | a, b \in \mathbf{F}_3\}$ is closed under addition and forms a field. Let us call it $\mathbf{F}_9$. Find an element of order 8 in $\mathbf{F}_9^\times$.

5. Let F be a field, and consider matrices

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \qquad \text{and} \qquad B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

with entries in F. If $b + c = 0$, show that $BA = A^{-1}B$. If, moreover, $\det A = -\mathrm{tr}\, A = 1$, show that $A^3 = I$. Exhibit a subgroup of $GL_2(\mathbf{F}_{13})$ isomorphic to the the group G of Exercise 1.

6. In $GL_2(\mathbf{F}_2)$, find a matrix A such that $A^2 = A + I$. Show that the set of matrices $\{0, I, A, A^2\}$ is closed under addition and forms a field (let us call it $\mathbf{F}_4$). Show that there are exactly two isomorphism between $\mathbf{F}_4^\times$ and the additive group of $\mathbf{F}_3$.

7. In $GL_2(\mathbf{F}_3)$, find a matrix J such that $J^2 = -I$. Show that the subset $\{aI + bJ | a, b \in \mathbf{F}_3\}$ is closed under addition and forms a field (let us call it $\mathbf{F}_9$). Find an element of order 8 in $\mathbf{F}_9^\times$.

8. Let $E = K[\tau]$ be a quadratic field extension with $\tau^2 = t \in K$. Consider an element $\alpha \in E$ with $\alpha \notin K$, say $\alpha = a + b\tau$. Further, let $f(X)$ be a cubic polynomial with coefficients in K.

(i) Show that $\alpha^2 + u\alpha + v = 0$ for suitable u, $v \in K$.

(ii) Show that $f(\alpha) \neq 0$, unless $f(c) = 0$ for some $c \in K$.

Linear Algebra and Geometry.

1. Let $\mathcal{U}$ and $\mathcal{V}$ be subspaces of a linear space $\mathcal{W}$ over some field K. Prove:

$$\dim\big(\mathcal{U} + \mathcal{V}\big) = \dim\mathcal{U} + \dim\mathcal{V} - \dim\big(\mathcal{U} \cap \mathcal{V}\big).$$

2. Let A be an $m \times n$ matrix over a field K. In the following, $\mathcal{C}$, $\mathcal{N}$, $\mathcal{R}$ refer to column-, null-, and row-space, respectively.

(i) Show that $\dim\mathcal{C}(A) = n - \dim\mathcal{N}(A)$.

(ii) Show that $\dim\mathcal{C}(A) = \dim\mathcal{R}(A)$.

3. Let K be a field with finitely many elemnts, $(F, +)$ be the cyclic subgroup generated by 1 in the additive group $(K, +)$, and $\{\alpha_1, \cdots, \alpha_m\}$ be a minimal set of genrators of $(K, +)$.

(i) Show that the set F is closed under multiplication and forms a field.

(ii) Show that $\{\alpha_1, \cdots, \alpha_m\}$ is a basis of K as linear space over F.

(iii) Conclude that the number of elements in K is a prime power.

4. Let A be a real $n \times n$ matrix, $\mathcal{V} \subseteq \mathbf{R}^n$ a subspace, and $\mathcal{V}^\perp$ the orthocomplement of $\mathcal{V}$ in $\mathbf{R}^n$ (i.e., the set of vectors $\perp$ to $\mathcal{V}$).

(i) Show that $A = A^T$ if and only if $AX \bullet Y = X \bullet AY$ for any pair $X, Y \in \mathbf{R}^n$.

(ii) Show: $A\mathcal{V} \subseteq \mathcal{V}$ implies $A\mathcal{V}^\perp \subseteq \mathcal{V}^\perp$.

(iii) How does this relate the Corollary of §6 to the Spectral Theorem ?

5. A real symmetric $n \times n$ matrix A is called *positive definite* if $AX \bullet X > 0$ for all $X \in \mathbf{R}^n$.

(i) Show that A is positive definite if and only if all its eigenvalues are positive.

(ii) If A is a positive definite matrix, show that there another such matrix B such that $B^2 = A$.

6. Let G be a finite subgroup of $GL_n(\mathbf{R})$.

(i) Find a positive definite matrix A such that $M^T AM = A$ for all $M \in G$.
(Hint: Try sums $\sum N^T N$ for $N \in G$.)

(ii) Show that G is similar to a subgroup of $O(n)$, that is: find an invertible B such that BMB^{-1} is orthogonal for all $M \in G$.

7. Show: If the real symmetric $n \times n$ matrices A and B commute, they have an orthogonal set $V_1, \ldots, V_n$ of common eigenvectors.

(*Hint:* $(A - \lambda I)V = 0$ implies $(A - \lambda I)BV = 0$, so B defines a symmetric tranformation on $\mathcal{N}(A - \lambda I)$ and hence has an eigenvector there.)

8. For any column $V \in \mathbf{R}^3$ with $|V| = 1$, consider the symmetric matrix $S_V = 2\,V\,V^T - I$.

(i) Evaluating $S_V\,V$, as well as $S_V\,X$ for $X \in V^\perp$, deduce that S_V is a rotation. What axis, what angle ?

(ii) Given two unit-columns V and W, show that $V^\perp \cap W^\perp$ is an eigenspace for $R = S_V S_W$. What is the eigenvalue? What kind of transformation is R ?

(iii) If $V \bullet W = \cos\theta$, find the angle between W and RW. Under what condition is $S_V S_W = S_U$ for suitable U ?

Math 322, Midterm Test, Nov.1, 1993.

1. Show that $G = SL_2(\mathbf{F}_3)$ is a group of order 24 having only one element of order 2. Deduce that G is not isomorphic to S_4.

$GL_2(\mathbf{F}_3)$ has 48 elements, since there are $3^2-1=8$ (resp. $3^2-3=6$) choices for the first (resp. second) column of an invertible matrix. $SL_2(\mathbf{F}_3)$ has $48/2=24$, as it is the kernel of the surjective homomorphism $\det : GL_2(\mathbf{F}_3) \longrightarrow \mathbf{F}_3^\times$, with $|\mathbf{F}_3^\times| = 2$.

For $A \in SL_2(F)$ with $\mathrm{tr}\,(A) = t$, Cayley-Hamilton reads: $tA = A^2 + I$. If $A^2 = I$, this becomes $tA = 2I$, whence $t \neq 0$ and $A = (2/t)I$ — provided only that $1+1 \neq 0$ in F. For $F = \mathbf{F}_3$, this means $A = \pm 1$.

By contrast, S_4 has nine elements of order 2, six of type (ab) and three of type $(ab)(cd)$.

2. Let N be a normal subgroup of the finite group G, and suppose that $|N|$ is relatively prime to $|G:N|$. Prove that N is the only subgroup of order $|N|$.

Let $H \leq G$ be a subgroup of order $|N|$, and consider its image K under the canonical homomorphism $\psi : G \longrightarrow G/N$. Since K is a subgroup of G/N, Lagrange says that $|K|$ divides $|G:N|$. Since K is a homomorphic image (hence quotient group) of H, its order must also divide $|H| = |N|$. By the stipulated relative primeness, we conclude that $|K| = 1$. Therefore $K = 1$, which means $H \leq \ker\psi = N$, whence $H = N$ because of the equality of orders.

3. Show that A_7 has a subgroup isomorphic to S_5, but no subgroup isomorphic to Z_{10}.

Let $\tau \in S_7$ denote the transposition (67), and consider the map $T : S_5 \longrightarrow S_7$ given by $T(\sigma) = \sigma\tau^{j(\sigma)}$, where $j(\sigma)$ is taken from the "sign" $\varepsilon(\sigma) = (-1)^{j(\sigma)}$. T is a homomorphism because $j(\sigma_1\sigma_2) \equiv j(\sigma_1) + j(\sigma_2)$ mod 2, and because τ commutes with all $\sigma \in S_5$, whence $T(\sigma_1\sigma_2) = \sigma_1\sigma_2\tau^{j(\sigma_1)+j(\sigma_2)} = \sigma_1\tau^{j(\sigma_1)} \cdot \sigma_2\tau^{j(\sigma_2)}$. Moreover, $\sigma\tau^{j(\sigma)} = (1) \iff \sigma = \tau^{j(\sigma)} = (1)$, and T is injective. Finally, $T(\sigma) \in A_7$ always, since $\varepsilon(\sigma\tau^{j(\sigma)}) = \varepsilon(\sigma)(-1)^{j(\sigma)} = 1$.

Any $\pi \in S_7$ of order 10 would have to be the (disjoint) product of a 5-cycle with a single 2-cycle, since there is no room for more than one of each. Hence $\varepsilon(\pi) = -1$, and $\pi \notin A_7$.

4. In $GL_2(\mathbf{F}_5)$, find a matrix J such that $J^2 = 2I$. Show that the set $E = \{aI + bJ | a, b \in \mathbf{F}_5\}$ of matrices over $\mathbf{F}_5$ forms a field of 25 elements.

For J, take any matrix of trace 0 and determinant -2 (lots of choice). In E we have the following formulas for addition and multiplication: $(aI+bJ)+(a'I+b'J) = (a+a')I+(b+b')J$ and $(aI+bJ)\cdot(a'I+b'J) = (aa'+2bb')I+(ab'+a'b)J$. Hence E is closed under both of these operations. Associativity and distributivity are inherited from the world of matrices, commutativity of multiplication is clear from the formula.

To see the existence of multiplicative inverses, note that $(aI+bJ)(a-bJ) = (a^2-2b^2)I$. Hence $aI+bJ$ fails to be invertible only if $a^2 - 2b^2 = 0$ in $\mathbf{F}_5$. This is impossible for $b \neq 0$, or else $(a/b)^2 = 2$ would contradict the fact that 1 and 4 are the only squares mod 5. Hence $a^2 - 2b^2 = 0$ happens only if $aI + bJ = 0$. All other elements of E are invertible, and E is a field. It has as many elements as there are pairs (a, b), since I and J are independent.

5. For every integer $a \in \mathbf{Z}$, prove that $a^5 \equiv a$ modulo 5, $a^{11} \equiv a$ modulo 11, and $a^{21} \equiv a$ modulo 55.

By the "Little Fermat", $b^{p-1} = 1$ in $\mathbf{F}_p$ for any $b \neq 0$. Hence $b^m = b$ for every $b \in \mathbf{F}_p$ (including $b = 0$), whenever $m = 1 + k(p-1)$ with $k \in Z$. In other words, $a^m \equiv a$ modulo p, for every $a \in Z$, whenever $m \equiv 1$ mod $(p-1)$.

Now if m satisfies this condition for two different primes p and q (e.g. $m = 21$, $p = 5$, $q = 11$), it follows that $(a^m - a)$ is divisible by both p and q, for every $a \in \mathbf{Z}$.

(Incidentally, for a "public key code", we need an m with a nifty factorization $m = sr$, to scramble with s and restore with r. Here is one way to get it: writing $(p-1)(q-1) = abd$ with $(a, b) = 1$, put $m = (ax + by)(au + bv)$ with $xu \equiv a^{-2}$ mod b and $yv \equiv b^{-2}$ mod a. Then $m \equiv 1$ mod ab, hence mod p-1 as well as mod q-1.)

THE UNIVERSITY OF BRITISH COLUMBIA

Sessional Examinations – December 1993

MATH 322 (Algebra I) Time: $2\frac{1}{2}$ hours

Part A. Five Questions = 75 Points.

Each of these counts for 15% of your grade.

1. Let K be an abelian group (written additively) with generators x, y, z and relations

$$10y + 5z = 5x + 10z = 10x + 5y = 0.$$

a) Show that $H = 5K$ is cyclic of order 9. (Note: H has generators $u = 5x$, $v = 5y$, $w = 5z$.)
b) How many elements of order 5 are there in K? Justify your answer.

2. Consider a finite subgroup $G < GL_n(\mathbf{R})$, where n is odd, and put $G_0 = G \cap SL_n(\mathbf{R})$.
a) Show that $\det \alpha = \pm 1$ for all $\alpha \in G$; using this, define a homomorphism $\psi : G \longrightarrow SL_n(\mathbf{R})$ whose kernel has order ≤ 2.
b) Show that either $G = \pm G_0$ or G is isomorphic to a subgroup of $SL_n(\mathbf{R})$.

3. Let G be a group of order 12 with more than 2 elements of order 3.
a) How many subgroups of order 4 does G have? Justify your answer.
b) Show that G has no subgroup of order 6.

4. Let F be a field of p elements, where p is an odd prime.
a) Show: if $a \in F^\times$ is a square, then $a^{(p-1)/2} = 1$.
b) Suppose that $(p-1)/2$ is odd. Show: the set of matrices of the form

$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix} = a \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + b \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},$$

with a, $b \in F$ not both zero, constitutes a group.

5. Let G denote S_4 or the octahedral group (take your pick).
a) Show that the Sylow 2-groups of G are dihedral.
b) How many are there, and what is their intersection? Justify your answer.

Part B. A Short Essay = 25 Points.

This should fit into one loosely typed page, but length is not essential.

6. Sketch some of the arguments used in the proof of ONE of the following 3 theorems. You may outline the whole proof or dwell on some salient aspect(s): the object of this exercise is to show your understanding of a larger context.

(i) Every finite subgroup of $GL_n(\mathbf{R})$ is similar (i. e., conjugate) to a subgroup of $O(n)$.

(ii) Every finite abelian group is isomorphic to a direct product of cyclic groups.

(iii) For every finite group G and every prime p dividing $|G|$, the set $\mathrm{Syl}_p(G)$ has cardinality $1 + pk$ (for suitable $k \in \mathbf{Z}$), and G acts on it transitively by conjugation.