Math 501, Fall 1994, Exercises.

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

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

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

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

Write out the multiplication table for G.

3. 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 $\mathbf{F}_3$.

4. 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 $\mathbf{F}_9^\times$.

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

6. 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 $c \in K$.

7. A field E is *constructible* over K if there is a finite chain of fields $K = E_0 \subset E_1 \subset \cdots \subset E_m = E$ such that E_i is quadratic over E_{i-1} for $i = 1, \ldots, m$.
(i) Using (6), show that a cubic polynomial with coefficients in K, not having a root in K, cannot have a root in any constructible extension of K.
(ii) With $\alpha = 2\cos 20°$, find a cubic polynomial $f(x)$ with rational coefficients such that $f(\alpha) = 0$, and show that α does not lie in any constructible extension of $\mathbf{Q}$.

8. Let $G \subset GL_3(\mathbf{F}_2)$ be the subgroup consisting of those matrices which have $[0, 0, 1]$ as their last row. Show that G is a group of order 24, isomorphic to the group S_4 of all permutations of 4 letters, but not isomorphic to $SL_2(\mathbf{F}_3)$.

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: $A = A^T$ and $A\mathcal{V} \subseteq \mathcal{V}$ 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 ?