VIGRE Algebra QR Review, October 28, 2002

Summary of Session

The sequence described last time

1
1 1
2 1
1 2 1 1
1 1 1 2 2 1
3 1 2 2 1 1
1 3 1 1 2 2 2 1
1 1 1 3 2 1 3 2 1 1
3 1 1 3 1 2 1 1 1 3 1 2 2 1
...

was "solved." Each row is a description of the preceding row, in a certain sense. E.g., the row 2 1 consists of one 2 and one 1, which leads to 1 2 1 1 for the next row. More precisely, each maximal string of consecutive entries that are the same in one row, e.g., b occurrences of the number a ($a\ a\ \ldots\ a$) generate an occurrence of $b\ a$ in the following row. The last row shown would generate: one 3, two 1's, one 3, one 1, one 2, three 1's, one 3, one 1, two 2's, and one 1 or: 1 3 2 1 1 3 1 1 1 2 3 1 1 3 1 1 2 2 1 1.

The following question was posed: every year, in the United States, there is a date on which more people are born than on any other (so that date will be their birthday). The date varies but is easily described — it is always a Sunday. What is it this year? The answer is given at the end.

The following problems are from the list for October 28 — I am including solutions for all of these problems (not all of them were discussed in detail).

1. (a) Find the order of the group $\mathrm{GL}(2, \mathbb{F}_p)$ of invertible 2×2 matrices over a field with p elements.

(b) Explicitly describe a Sylow p-subgroup of $\mathrm{GL}(2, \mathbb{F}_p)$.

(c) Show that $\mathrm{GL}(2, \mathbb{F}_p)$ has a normal subgroup of index $p-1$. (Hint: the determinant map!).

(d) Now let U be the subgroup of $\mathrm{GL}(2, \mathbb{F}_p)$ of 2×2 upper triangular matrices. Prove that U is solvable.

Solution. Here is the solution to (a) generalized to the case of $\mathrm{GL}(n, \mathbb{F}_q)$. The idea is to choose the rows, say, one at a time, but so that they are independent. The number of choices for the first row is $q^n - 1$, since the row of all 0s is excluded. The number of choices for the second row is then $q^n - q$, since multiples of the first row are excluded. If the first k rows have already been chosen so as to be linearly independent, the number of choices for the $(k+1)$ st row is $q^n - q^k$, since q^k is the number of the elements in a k-dimensional vector space over $\mathbb{F}_q$, and linear combinations of the first k rows must be excluded. The number of choices for the last row will be $q^n - q^{n-1}$. The number of invertible matrices is then $\prod_{k=0}^{n-1}(q^n - q^k)$. In the problem here, $q = p$ and $n = 2$, so the answer is $(p^2-1)(p^2-p)$.

For part (b), first note that the highest power of p dividing the order of the group is p, so a Sylow p-subgroup will have order p. Thus, the problem becomes to find an explicit example of a 2×2 matrix of order p. One example is $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. One can check easily by induction that the kth power is $\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$, which first vanishes for $k = p$, since $p = 0$ in the field. The sum of I with any nilpotent matrix N (since the size is 2×2, $N^2 = 0$) will work: since I and N commute and $N^2 = 0$, $(I+N)^p = I^p + N^p$ (the intermediate binomial coefficients are 0) $= I + 0 = I$. The Sylow p-subgroup is generated by the element of order p one chooses.

For (c), note that the determinant map is a group homomorphism onto the multiplicative group with $p-1$ elements (the diagonal matrix with a and 1 on the diagonal maps to a) Therefore the kernel, which is $\mathrm{SL}(2, \mathbb{F}_p)$ has index $p-1$.

For part (d), check that the map sending invertible matrices of the form $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ to the pair of diagonal entries (a, c) (thought of as an element of the product of two copies of the multiplicative group of F) is a homomorphism of the group onto an abelian group. The kernel consists of all matrices of the form $M_b = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$, and since $M_b M_{b'} = M_{b+b'}$, the kernel is isomorphic with the additive group of the field, and is therefore abelian. Since the group is an extension of an abelian group by an abelian group, it is solvable. (More generally, the group of $n \times n$ upper triangular matrices over any field is solvable.)

2. Let F be a finite field of q elements of char. $p > 0$, and let $a \in F - \{0\}$. Prove that $g(x) = x^q - x - a$ has no roots in F and that its splitting field over F is an extension of degree p. [The examiners gave this hint: There is a root r in some extension field. Prove that $\{r + c : c \in F\}$ is then the complete set of roots of $g(x)$. The easiest solution of this problem does not use this hint.]

Solution. The field with q elements is the splitting field of $x^q - x$: for r in it, $r^q - r - a = 0 - a = -a \neq 0$, so the equation has no root in F. An extension of F of degree p will be, as an F-vector space, the direct sum of p copies of F, and will therefore have q^p elements (**not** qp). It will suffice to show that all roots of the equation are in the Galois field L with q^p elements: because this field has degree p over F, and any intermediate field has degree dividing p over F, i.e., 1 or p, there are no proper intermediate fields. Since the equation has no roots in F, it will follow that the splitting field is L. To see that a root r is in L, it suffices to see that $r^{q^p} = r$, for L is the splitting field of $x^{q^p} - x$. But the qth power map, applied to the set of roots the equation, is the same as the map that adds a to each element: $r^q = r + a$ because r is a root of the equation. It follows by induction that $r^{q^i} = r + ia$ for all i. Thus, $r^{q^p} = r + pa = r + 0 = r$, as required.

3. Let $\mathbb{F}_q$ be the finite field with q elements, and let $G = \mathrm{GL}_2(\mathbb{F}_q)$ be the group of 2×2 invertible matrices with elements in $\mathbb{F}_q$. Let $V = \mathbb{F}_q^2$ be the vector space of 2×1 column

vectors over $\mathbb{F}_q$.

(a) Explain how G acts naturally on the set $\mathbb{P}$ of all one-dimensional subspaces of V.

(b) Let $W \subseteq V$ be the subspace spanned by $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$. Find the stabilizer of $W \in \mathbb{P}$ in G, i.e., the subgroup S of G whose elements fix W.

(c) What is the index of S in G?

Solution. (a) More generally, for any field K, $\mathrm{GL}(n,\ K)$ acts on the set of all d-dimensional subspaces of K^n. The value of a linear transformation on a subspace is simply the image of the subspace under that linear transformation. The image of a basis for the subspace will be a basis for the image: since the transformation is invertible, it has no kernel, and preserves dimensions. (This action is transitive. Given two subspaces of dimension d, choose a basis for each. Extend each basis to a full basis for K^n. Then there is a unique invertible linear transformation taking the first full basis to the second, and it will map the first given subspace to the second.)

For part (b), the condition for an invertible 2×2 matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ to be in the stabilizer is simply that its value on $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ (multiply on by the matrix on the left), which is $\begin{pmatrix} a \\ c \end{pmatrix}$, be in the span of $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$, i.e., that $c = 0$. Thus, the stabilizer consists of all matrices of the form $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ (i.e., upper triangular matrices) which are invertible (equivalently, such that $ad \neq 0$). This does not depend on the field.

The order of the stabilizer is $(q-1)^2 q$ (there are $q-1$ choices for each of a, d, and q choices for b). Its index is therefore $\big((q^2-1)(q^2-q)\big)/\big((q-1)^2 q\big) = q+1$. This should be the same as the number of lines through the origin (the cardinality of the orbit): this is correct, because each line except the span of $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ is uniquely spanned by a vector of the form $\begin{pmatrix} a \\ 1 \end{pmatrix}$ (which is a second way of solving the problem).

4. As a function of q, how many nilpotent 2×2 matrices are there over a finite field with q elements?

Solution. There are many ways to do the counting. An $n \times n$ matrix is nilpotent if and only if the char. polynomial is x^n: here, $n = 2$, and so the condition for nilpotence is that the trace and determinant be 0. If the entry on the upper left is a, one can consider two cases. If $a \neq 0$, then the matrix must have the form $\begin{pmatrix} a & b \\ -a^2/b & -a \end{pmatrix}$: the choice of $-a$ is dictated by the fact that the trace is 0, and the choice of $-a^2/b$ is then dictated by the fact that the determinant is 0. Here, b must be nonzero. So there are $(q-1)^2$ such matrices. The number of nilpotent matrices with $a = 0$ is also easy to count: these have the form $\begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}$ with $bc = 0$. Thus, either $b = 0$, $c = 0$ or both, and this gives $2q - 1$ additional matrices. The total number of nilpotent matrices is $(q-1)^2 + 2q - 1 = q^2$. [Alternate: a matrix is nilpotent iff it is similar to 0 or $J = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ (these are the only two possible rational forms). 0 is similar only to itself. An invertible matrix A is in the stabilizer H of J under conjugation iff $AJ = JA$. It is then easy to see that A must be lower triangular with a constant $\neq 0$ on the diagonal, so that $|H| = (q-1)^2 q$. Thus, H has index $q^2 - 1$, the number of conjugates of A. Thus, there are $(q^2 - 1) + 1 = q^2$ nilpotent matrices.]

5. A finite field F has 81 elements. How many solutions are there to the equation $x^{25} = 1$ in this field?

Solution. The multiplicative group of the field has order 80 and is abelian (it is cyclic, but we do not need to use that). It follows that is the product of $\mathbb{Z}_5$ with a group of order 16. An element satisfies $x^{25} = 1$ if and only if its order divides 25, and so its order must be 1, 5 or 25. But its order must divide 80, so that the roots of this equation are actually the same as the elements of order 1 or 5. The number of such elements is precisely the cardinality of the unique Sylow 5-subgroup, which is 5.

6. Show that the group $\mathrm{SL}(n, \mathbb{Z})$ of $n \times n$ matrices over the integers with determinant 1 is finitely generated.

Solution. Such a matrix can be made diagonal by elementary row and column operations. But an elementary row (resp., column) operation can be achieved by performing the operation on the identity matrix, producing a so-called *elementary matrix*, which has precisely one nonzero entry off the main diagonal and 1s on the main diagonal, and then multiplying by the elementary matrix on the left (resp., right). Thus, the elementary matrices together with the diagonal matrices with determinant one generate. The latter can have only 1 and -1 (-1 must occur an even number of times) on the diagonal, and so there are only finitely many. One doesn't need all the elementary matrices, however: e.g., one can add n times a row to another by adding 1 times the row to the other, repeating n times. (Rephrasing: let $E_{i,j}(t)$ be the elementary matrix with t as the only possible nonzero entry off the diagonal, and in the i, j spot, $i \neq j$. Then $E_{i,j}(n) = E_{i,j}(1)^n$ for all $n \in \mathbb{Z}$.) Thus, the elementary matrices with a single 1 off the main diagonal together with the diagonal matrices with only 1 and -1 (-1 an even number of times) on the main diagonal generate.

7. An 11×11 matrix M over a field F has square 0. Find all the possibilities for the Jordan form of M. Does the number of possible Jordan forms depend on F?

Solution. For the square to be 0, all eigenvalues must be zero, and the Jordan blocks all of size 1 or 2. This condition is necessary and sufficient. The form is completely determined by the number k of size 2 Jordan blocks, which must satisfy $0 \leq k \leq 5$: other blocks must be size 1. There are therefore 6 possible Jordan forms, independent of F.

The largest number of people are born on the Sunday of the fall time change: that day has 25 hours. The birth rate is not constant: it is larger nine months after the winter months. The date of the time change is also nine months after the end of January, so the extra hour in that day is decisive. This year it was Sunday, October 27.