

HOMEWORK 8 Solutions  
Math100B UCSD Winter 2002

1. In class we saw a formula for the size of  $\text{GL}_n(\mathbf{F}_p)$  and  $\text{SL}_n(\mathbf{F}_p)$ .

a) Compute the size of  $\text{GL}_n(\mathbf{F}_5)$  and  $\text{SL}_n(\mathbf{F}_5)$  for  $n = 1, 2, 3, 4$ .

b) Prove the group of strictly upper-triangular matrices in  $\text{GL}_n(\mathbf{F}_p)$  (1's on main diagonal, 0's below, arbitrary stuff above main diagonal) is a  $p$ -Sylow subgroup. Are these matrices also a  $p$ -Sylow subgroup of  $\text{SL}_n(\mathbf{F}_p)$ ?

Solution a) Here is a table, where we use the formulas

$$\#\text{GL}_n(\mathbf{F}_p) = (p^n - 1)(p^n - p)(p^n - p^2) \cdots (p^n - p^{n-1}), \quad \#\text{SL}_n(\mathbf{F}_p) = \frac{\#\text{GL}_n(\mathbf{F}_p)}{p - 1}$$

with  $p = 5$  and  $n = 1, 2, 3, 4$ .

$n$	$\#\text{GL}_n(\mathbf{F}_5)$	$\#\text{SL}_n(\mathbf{F}_5)$
1	4	1
2	480	120
3	1488000	372000
4	1106064000000	290160000000

b) We are looking at matrices of the form

$$\begin{pmatrix} 1 & * & * & \cdots & * & * \\ 0 & 1 & * & \cdots & * & * \\ 0 & 0 & 1 & \cdots & * & * \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & * \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix},$$

where  $*$  means anything from  $\mathbf{F}_p$  can be put there. We saw in class that such matrices form a group under multiplication.

Since each  $*$  has  $p$  choices, and different  $*$ 's are unrelated, the number of such matrices is  $p^N$ , where  $N$  is the number of  $*$ 's. Adding up the number of them column by column, we have

$$N = 1 + 2 + \cdots + (n - 2) + (n - 1) = \frac{n(n - 1)}{2}.$$

Therefore the number of strictly upper triangular  $n \times n$  matrices over  $\mathbf{F}_p$  is  $p^{n(n-1)/2}$ .

Meanwhile, the size of a  $p$ -Sylow subgroup of  $\text{GL}_n(\mathbf{F}_p)$  is obtained by pulling out the biggest power of  $p$  from  $\#\text{GL}_n(\mathbf{F}_p)$ . Look at the formula for  $\#\text{GL}_n(\mathbf{F}_p)$ . Since  $p^n - p^i$ , for  $0 \leq i \leq n - 1$ , is divisible by  $p^i$  but not by  $p^{i+1}$ , we see the biggest power of  $p$  in  $\#\text{GL}_n(\mathbf{F}_p)$  is

$$p^0 \cdot p^1 \cdot p^2 \cdots p^{n-1} = p^{n(n-1)/2}.$$

2. This is a review exercise on inverse functions and assorted algebraic structures, to be sure you understand the basic idea here once and for all.

a) Let  $f: X \rightarrow Y$  be a map of sets which is a bijection (that is,  $f$  is one-to-one and onto). Define the inverse function  $f^{-1}: Y \rightarrow X$ , by describing how the value  $f^{-1}(y)$  is determined for  $y \in Y$ .

b) Let  $f: G_1 \rightarrow G_2$  be a group homomorphism which is a bijection. Prove the inverse of  $f$  is a group homomorphism. That is, prove  $f^{-1}(gg') = f^{-1}(g)f^{-1}(g')$  for all  $g, g' \in G_2$ .

c) Let  $f: R_1 \rightarrow R_2$  be a ring homomorphism which is a bijection. Prove the inverse of  $f$  is a ring homomorphism. That is,  $f^{-1}(1) = 1$ ,  $f^{-1}(r + r') = f^{-1}(r) + f^{-1}(r')$ , and  $f^{-1}(rr') = f^{-1}(r)f^{-1}(r')$  for all  $r, r' \in R_2$ .

d) Let  $f: V_1 \rightarrow V_2$  be a linear map of vector spaces over  $F$  which is a bijection. Prove the inverse of  $f$  is linear. That is,  $f^{-1}(v + v') = f^{-1}(v) + f^{-1}(v')$  and  $f^{-1}(cv) = cf^{-1}(v)$  for all  $v, v' \in V_2$  and  $c \in F$ .

Solution a) For  $y \in Y$ ,  $f^{-1}(y)$  is the unique  $x \in X$  such that  $f(x) = y$ ;  $x$  exists since  $f$  is onto, and  $x$  is unique since  $f$  is one-to-one.

b,c,d) I will prove all of these by a uniform method. Suppose  $X$  and  $Y$  are sets and  $*_1, *_2$  are binary operations on  $X$  and  $Y$  respectively, and  $f: X \rightarrow Y$  is a “\*-homomorphism,” *i.e.*,

$$f(x *_1 x') = f(x) *_2 f(x')$$

for all  $x, x' \in X$ . For instance, we can use groups and group homomorphisms, rings and either ring addition or ring multiplication, and vector spaces and vector space addition.

Let's show that, when  $f$  is a bijection, the inverse  $f^{-1}$  is a \*-homomorphism in the other direction:

$$f^{-1}(y *_2 y') = f^{-1}(y) *_1 f^{-1}(y')$$

for all  $y, y' \in Y$ .

Both sides are elements of  $X$ , so we can show they are equal by taking  $f$  of both sides and checking the results are equal (because  $f$  is one-to-one). Well, since  $f$  “undoes”  $f^{-1}$ ,

$$f(f^{-1}(y *_2 y')) = y *_2 y'.$$

Taking  $f$  of the other side, we have

$$f(f^{-1}(y) *_1 f^{-1}(y')) = f(f^{-1}(y)) *_2 f(f^{-1}(y')) = y *_2 y',$$

where the first equation uses the fact that  $f$  is a \*-homomorphism!

Since  $f^{-1}(y *_2 y')$  and  $f^{-1}(y) *_1 f^{-1}(y')$  have the same  $f$ -value, they are equal.

This settles all parts of the problem except for two things: that a bijective ring homomorphism satisfies  $f^{-1}(1) = 1$  and that a bijective linear map of vector spaces preserves scaling:  $f^{-1}(cv) = cf^{-1}(v)$ . These can be checked as above, by applying  $f$  to both sides, using the fact that  $f$  is either a ring homomorphism or a linear map to simplify the resulting right side, and seeing the end result on both sides is the same, so both sides were equal to begin with by injectivity of  $f$ .

3. Let  $\text{Pol}_n(F) = F + FT + \cdots + FT^n$  be the span of the powers  $1, T, \dots, T^n$ . One basis is  $1, T, \dots, T^n$ , so  $\text{Pol}_n(F)$  has dimension  $n + 1$ . For example,  $\text{Pol}_2(F)$  is 3-dimensional with basis  $\{1, T, T^2\}$ .

Consider differentiation  $D: \text{Pol}_n(F) \rightarrow \text{Pol}_n(F)$ , which is a linear map. (Yes, the image is really in  $\text{Pol}_{n-1}(F)$ , but think about it in  $\text{Pol}_n(F)$ .)

a) Write  $D: \text{Pol}_2(F) \rightarrow \text{Pol}_2(F)$ , as a matrix relative to the basis  $\{1, T, T^2\}$ .

b) Show  $\{T, T + 1, T^2 + T\}$  is also a basis of  $\text{Pol}_2(F)$ , and write the matrix for differentiation on  $\text{Pol}_2(F)$  relative to this basis. Be careful! For matrix calculations, all results should be expressed in coordinates for this (unusual) basis, not for the standard basis  $\{1, T, T^2\}$ .

c) Compute the characteristic polynomials of both matrices in (a) and (b). (Hint: the two characteristic polynomials must be the same, so if they are not you'll know there was an error somewhere.)

Solution a) Set  $e_1 = 1, e_2 = T, e_3 = T^2$ . Then

$$D(e_1) = 0, \quad D(e_2) = 1 = e_1, \quad D(e_3) = 2T = 2e_2,$$

so the matrix for  $D$  relative to  $\{1, T, T^2\}$  is

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix}.$$

Notice that the cube of this matrix is the zero matrix, which is consistent with the fact the differentiating a polynomial of degree at most 2 three times will give 0.

b) We know the space is 3-dimensional (because we already have the basis  $\{1, T, T^2\}$ ), so we can check the set  $\{T, T + 1, T^2 + T\}$  is a basis just by checking it spans; since it has size 3 it then must be linearly independent.

To see this set spans, it suffices to find the already known spanning set  $\{1, T, T^2\}$  inside the span of  $T, T + 1, T^2 + T$ . Well,

$$1 = (T + 1) - T, \quad T = T, \quad T^2 = (T^2 + T) - T.$$

Now we write the matrix for differentiation in this new basis. Let  $e_1 = T, e_2 = T + 1, e_3 = T^2 + T$ . Then

$$D(e_1) = 1 = e_2 - e_1, \quad D(e_2) = 1 = e_2 - e_1, \quad D(e_3) = 2T + 1 = e_1 + e_2,$$

so the matrix of  $D$  in this basis is

$$\begin{pmatrix} -1 & -1 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

c) The characteristic polynomials of both matrices is  $X^3$ . This is related to the fact that iterating differentiation three times on  $\text{Pol}_2(F)$  is the zero transformation (sending everything to 0).

4. For a polynomial  $f(T) \in \mathbf{F}_2[T]$ , set

$$A_f = \mathbf{F}_2[T]/(f(T)),$$

which is both a ring and an  $\mathbf{F}_2$ -vector space, of dimension  $\deg f$ . Let  $\varphi_2: A_f \rightarrow A_f$  be the Frobenius map. That is,  $\varphi_2$  is squaring on  $A_f$ , which is  $\mathbf{F}_2$ -linear.

Here are several polynomial choices for  $f$ :

$$T^2, \quad T^2 + 1, \quad T^2 + T + 1, \quad T^3 + 1, \quad T^3 + T + 1.$$

For each of these choices of  $f$ , do three things: factor  $f$  into irreducibles in  $\mathbf{F}_2[T]$  (use problem 1 on set 6 to find the low degree irreducibles), compute the matrix of  $\varphi_2$  on  $A_f$  relative to the basis of powers of  $T$  in  $A_f$ , and compute the characteristic polynomial of  $\varphi_2$ . Present your work cleanly.

Solution.

First we factor the polynomials.

Polynomial	Factorization
$T^2$	$T^2 = T \cdot T$
$T^2 + 1$	$(T + 1)^2$
$T^2 + T + 1$	$T^2 + T + 1$
$T^3 + 1$	$(T + 1)(T^2 + T + 1)$
$T^3 + T + 1$	$T^3 + T + 1$

We're asked to compute the matrix for squaring on  $A_f = \mathbf{F}_2[T]/(f(T))$ , relative to the basis of powers of  $T$  in  $A_f$ , which is the basis  $\{1, T, T^2, \dots, T^{d-1}\}$ , where  $d = \deg f$ . We proceed case by case.

First, with  $T^2$ , in  $\mathbf{F}_2[T]/(T^2)$  we use the basis  $e_1 = 1$  and  $e_2 = T$ . Then

$$\varphi_2(e_1) = 1 = 1 \cdot e_1 + 0 \cdot e_2, \quad \varphi_2(e_2) = T^2 = 0 = 0 \cdot e_1 + 0 \cdot e_2,$$

so

$$[\varphi_2] = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

The characteristic polynomial is  $(X - 1)X = X^2 + X$ . (It is not, notationally, a good idea to use  $T$  as the variable in the characteristic polynomial, since we're using  $T$  for an element of our space  $A_f$ .)

For the second polynomial,  $T^2 + 1$ , we use in  $\mathbf{F}_2[T]/(T^2 + 1)$  the basis  $e_1 = 1, e_2 = T$ . (Warning: the algebraic properties of  $T$  in  $\mathbf{F}_2[T]/(T^2)$  and in  $\mathbf{F}_2[T]/(T^2 + 1)$  are not the same, so the fact that we write " $e_2 = T$ " in both cases does *not* mean the sets  $\mathbf{F}_2[T]/(T^2)$  and  $\mathbf{F}_2[T]/(T^2 + 1)$  have the "same" basis! These are two different rings.)

In  $\mathbf{F}_2[T]/(T^2 + 1)$ ,

$$\varphi_2(e_1) = 1 = e_1, \quad \varphi_2(e_2) = T^2 = 1 = e_1,$$

so

$$[\varphi_2] = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix},$$

whose characteristic polynomial is  $(X - 1)X = X^2 + X$ .

For the third space,  $\mathbf{F}_2[T]/(T^2 + T + 1)$ , we use the basis  $e_1 = 1$  and  $e_2 = T$ , and find

$$\varphi_2(e_1) = 1 = e_1, \quad \varphi_2(e_2) = T^2 = 1 + T = e_1 + e_2,$$

so

$$[\varphi_2] = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

whose characteristic polynomial is  $(X - 1)^2 = X^2 + 1$ .

For the fourth space,  $\mathbf{F}_2[T]/(T^3 + 1)$ , we use the basis  $e_1 = 1$ ,  $e_2 = T$ , and  $e_3 = T^2$ . Working modulo  $T^3 + 1$ ,

$$\varphi_2(e_1) = 1 = e_1, \quad \varphi_2(e_2) = T^2 = e_3, \quad \varphi_2(e_3) = T^4.$$

Since  $T^3 = 1$ ,  $T^4 = T$ , so  $\varphi_2(e_3) = e_2$ . Thus

$$[\varphi_2] = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$

whose characteristic polynomial is  $(X - 1)(X^2 - 1) = (X + 1)^3$ .

For the last space,  $\mathbf{F}_2[T]/(T^3 + T + 1)$ , we use the basis  $e_1 = 1$ ,  $e_2 = T$ , and  $e_3 = T^2$ . Working modulo  $T^3 + T + 1$ ,

$$\varphi_2(e_1) = 1 = e_1, \quad \varphi_2(e_2) = T^2 = e_3, \quad \varphi_2(e_3) = T^4.$$

Since  $T^3 = T + 1$ ,  $T^4 = T^2 + T$ , so  $\varphi_2(e_3) = e_2 + e_3$ . Thus

$$[\varphi_2] = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix},$$

whose characteristic polynomial is  $(X - 1)(X^2 - X - 1) = (X + 1)(X^2 + X + 1) = X^3 + 1$ .

5. (Composition and differentiation) The purpose of this final exercise is to illustrate that the linear algebra idea of thinking about numbers as scaling functions (that is, the number  $t$  is viewed as the function “scale by  $t$ ”) gives the chain rule of calculus a simple algebraic form.

Let  $f: \mathbf{R} \rightarrow \mathbf{R}$  be a differentiable function. Define a new function  $df: \mathbf{R}^2 \rightarrow \mathbf{R}^2$  by

$$(df)(x, y) = (f(x), f'(x)y).$$

The idea here is to think about the number  $f'(x)$  as the function “scale by  $f'(x)$ ”; the role of the second variable  $y$  is to make the scaling effect visible, since  $y$  is replaced with  $f'(x)y$ .

a) For the function  $f(x) = x^3 - 5x + 1$ , compute  $(df)(2, 8)$ .

b) Given two differentiable functions  $f, g: \mathbf{R} \rightarrow \mathbf{R}$ , we get two functions  $df, dg: \mathbf{R}^2 \rightarrow \mathbf{R}^2$ . Compute the composite function  $dg \circ df: \mathbf{R}^2 \rightarrow \mathbf{R}^2$ , and then explain why the chain rule of calculus is essentially equivalent to the nice formula

$$d(g \circ f) = dg \circ df.$$

Pretty neat!

Solution. a) We have  $f'(x) = 3x^2 - 5$ , so

$$(df)(2, 8) = (f(2), f'(2)8) = (-1, 56).$$

b) Let  $h = g \circ f$ . Then

$$(dh)(x, y) = (h(x), h'(x)y) = (g(f(x)), (g \circ f)'(x)y).$$

Meanwhile,

$$\begin{aligned} ((dg) \circ (df))(x, y) &= (dg)((df)(x, y)) \\ &= (dg)(f(x), f'(x)y) \\ &= (g(f(x)), g'(f(x))f'(x)y). \end{aligned}$$

Comparing with  $(dh)(x, y) = (d(f \circ g))(x, y)$ , we see  $d(g \circ f)$  and  $dg \circ df$  at any point  $(x, y)$  always have the same first coordinate. For them to be equal functions therefore is the same as always having the same second coordinate, *i.e.*,

$$(g \circ f)'(x)y = g'(f(x))f'(x)y$$

for all  $x$  and  $y$ . Taking  $y = 1$ , this implies the usual chain rule formula. Conversely, from the chain rule we just multiply both sides by  $y$  to get the above formula. Voilà.