

# MATH511A Final Exam · Due Monday December 10

Martin Leslie

## 1. Symplectic Spaces

Let  $\mathbb{F}$  be a field. A bilinear form  $\langle \cdot, \cdot \rangle$  on an  $\mathbb{F}$ -vector space  $W$  is said to be *alternating* if  $\langle v, w \rangle = -\langle w, v \rangle$  for all  $v, w \in W$ , and *nondegenerate* if for all nonzero  $v \in W$  there exists  $w \in W$  such that  $\langle v, w \rangle \neq 0$ . A nondegenerate alternating form is called a symplectic form.

- (a) For each  $i = 1, \dots, n$  let  $V_i$  be an  $\mathbb{F}$ -vector space equipped with a bilinear form  $\langle \cdot, \cdot \rangle_i$ . Show that there exists a unique bilinear form  $\langle \cdot, \cdot \rangle$  on the vector space  $V_1 \oplus \dots \oplus V_n$  such that
- (i)  $\langle v, v' \rangle = \langle v, v' \rangle_i$  if  $v, v'$  are both in  $V_i$ , and
  - (ii)  $\langle v, v' \rangle = 0$  if  $v \in V_i$  and  $v' \in V_j$  with  $i \neq j$ .

For  $v, v' \in V_1 \oplus \dots \oplus V_n$  we know that  $v = (v_1, \dots, v_n) = v_1 + \dots + v_n$  and  $v' = (v'_1, \dots, v'_n) = v'_1 + \dots + v'_n$  where  $v_i, v'_i \in V_i$  and we are identifying  $V_i$  with  $\{0\} \oplus \dots \oplus \{0\} \oplus V_i \oplus \{0\} \oplus \dots \oplus \{0\}$ . So if such a bilinear form exists it must satisfy

$$\begin{aligned} \langle v, v' \rangle &= \langle v_1 + \dots + v_n, v'_1 + \dots + v'_n \rangle \\ &= \sum_{i=1}^n \sum_{j=1}^n \langle v_i, v'_j \rangle \\ &= \sum_{i=1}^n \langle v_i, v'_i \rangle. \end{aligned}$$

So we now define our putative form by this equation and check that it is in fact a bilinear form. If it is, then it is unique because we have shown that any bilinear form with properties (i) and (ii) must be defined by this equation.

Now for  $u, v, u', v' \in V_1 \oplus \dots \oplus V_n$  and  $c \in \mathbb{F}$  we check:

- (i) Linearity in first coordinate.

$$\begin{aligned} \langle v + u, v' \rangle &= \langle (v_1 + u_1, \dots, v_n + u_n), (v'_1, \dots, v'_n) \rangle \\ &= \sum_{i=1}^n \langle (v_i + u_i), v'_i \rangle_i \\ &= \sum_{i=1}^n (\langle v_i, v'_i \rangle_i + \langle u_i, v'_i \rangle_i) \\ &= \sum_{i=1}^n \langle v_i, v'_i \rangle_i + \sum_{i=1}^n \langle u_i, v'_i \rangle_i \\ &= \langle v, v' \rangle + \langle u, v' \rangle \end{aligned}$$

$$\begin{aligned} \langle cv, v' \rangle &= \langle (cv_1, \dots, cv_n), (v'_1, \dots, v'_n) \rangle \\ &= \sum_{i=1}^n \langle cv_i, v'_i \rangle_i \\ &= c \sum_{i=1}^n \langle v_i, v'_i \rangle_i \\ &= c \langle v, v' \rangle \end{aligned}$$

(ii) Linearity in the second coordinate.

$$\begin{aligned}
 \langle v, v' + u' \rangle &= \langle (v_1, \dots, v_n), (v'_1 + u'_1, \dots, v'_n + u'_n) \rangle \\
 &= \sum_{i=1}^n \langle v_i, v'_i + u'_i \rangle_i \\
 &= \sum_{i=1}^n (\langle v_i, v'_i \rangle_i + \langle v_i, u'_i \rangle_i) \\
 &= \sum_{i=1}^n \langle v_i, v'_i \rangle_i + \sum_{i=1}^n \langle v_i, u'_i \rangle_i \\
 &= \langle v, v' \rangle + \langle v, u' \rangle
 \end{aligned}$$

$$\begin{aligned}
 \langle v, cv' \rangle &= \langle (v_1, \dots, v_n), (cv'_1, \dots, cv'_n) \rangle \\
 &= \sum_{i=1}^n \langle v_i, cv'_i \rangle_i \\
 &= c \sum_{i=1}^n \langle v_i, v'_i \rangle_i \\
 &= c \langle v, v' \rangle
 \end{aligned}$$

So our map is bilinear, so by above discussion is the unique bilinear form with the desired properties.

(b) If  $H$  is a 2-dimensional  $\mathbb{F}$ -vector space with a symplectic bilinear form  $\langle \cdot, \cdot \rangle$ , prove that  $H$  has a basis with respect to which the bilinear form has the matrix

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

Say  $\{e_1, e_2\}$  is a basis for  $H$ . Then  $\langle e_1, e_1 \rangle = -\langle e_1, e_1 \rangle$  by the alternating property so  $\langle e_1, e_1 \rangle = 0$  and similarly  $\langle e_2, e_2 \rangle = 0$ . Also nondegeneracy means  $\langle e_1, e_2 \rangle \neq 0$  so since  $\langle e_1, e_2 \rangle = -\langle e_2, e_1 \rangle$  one of these must be positive. Switching  $e_1$  and  $e_2$  if necessary, we may assume that  $\langle e_2, e_1 \rangle > 0$ . Then let

$$u = \frac{e_1}{\sqrt{\langle e_2, e_1 \rangle}} \text{ and } v = \frac{e_2}{\sqrt{\langle e_2, e_1 \rangle}}.$$

Now  $\{u, v\}$  is a basis for  $H$  since it is just a rescaling of  $\{e_1, e_2\}$  by a nonzero factor. And  $\langle u, u \rangle = 0$ ,  $\langle u, v \rangle = -1$ ,  $\langle v, u \rangle = 1$ ,  $\langle v, v \rangle = 0$  as desired.

(c) If  $W$  is a finite dimensional  $\mathbb{F}$ -vector space with a symplectic bilinear form prove that  $W$  is isomorphic to the orthogonal direct sum

$$H \oplus H \oplus \dots \oplus H$$

of  $m$  copies of  $H$ , for some integer  $m$ .

First we show that if  $W$  is  $n$ -dimensional with  $n$  odd that it cannot have a symplectic bilinear form by showing that any alternating form on  $W$  is degenerate. Recall that a form is degenerate iff the matrix representing it has determinant zero. But the matrix representing an alternating form will have  $a_{ij} = -a_{ji}$ , that is be skew-symmetric. So if  $A$  is the matrix representing the alternating form then  $\det(A) = \det(A^t) = (-1)^n \det(A)$ . So if  $n$  is odd then  $\det(A) = 0$ .

Thus if  $W$  has a symplectic bilinear form then  $n = 2m$  is even. We prove the claim in the question by induction on  $n$ . The  $n = 2$  case is part (b). For the inductive case say  $H$  has basis  $\{e_1, \dots, e_n\}$ . Then taking  $e_1$ , the nondegeneracy of the form means there exists some  $e_i$  with  $\langle e_1, e_i \rangle \neq 0$ . Relabeling the basis vectors (and switching  $e_1, e_i$  if necessary) we may assume that  $\langle e_2, e_1 \rangle > 0$ . So then set

$$u_1 = \frac{e_1}{\sqrt{\langle e_2, e_1 \rangle}} \text{ and } u_2 = \frac{e_2}{\sqrt{\langle e_2, e_1 \rangle}}.$$

For  $i = 3, \dots, n$  set

$$u_i = e_i - \langle u_2, e_i \rangle u_1 + \langle u_1, e_i \rangle u_2.$$

Then for  $i \geq 3$ ,

$$\langle u_1, u_i \rangle = \langle u_1, e_i \rangle - \langle u_2, e_i \rangle \langle u_1, u_1 \rangle + \langle u_1, e_i \rangle \langle u_1, u_2 \rangle = \langle u_1, e_i \rangle - \langle u_1, e_i \rangle = 0$$

and

$$\langle u_2, u_i \rangle = \langle u_2, e_i \rangle - \langle u_2, e_i \rangle \langle u_2, u_1 \rangle + \langle u_1, e_i \rangle \langle u_2, u_2 \rangle = \langle u_2, e_i \rangle - \langle u_2, e_i \rangle = 0.$$

Now since  $\{u_1, \dots, u_n\}$  is obtained from the basis  $\{e_1, \dots, e_n\}$  by scaling and adding multiples of other basis elements to each element it is also a basis for  $W$ . Let  $U$  be the vector space generated by  $\{u_1, u_2\}$  and  $V$  be the vector space generated by  $\{u_3, \dots, u_n\}$ . Then  $U + V = W$  and  $U \cap V = \{0\}$  so  $W = U \oplus V$  as vector spaces. Also, for  $u \in U$  and  $v \in V$ ,  $\langle u, v \rangle = 0$  so  $W = U \oplus V$  in the sense of part (a).

Now  $V$  is an  $(n - 2)$ -dimensional vector space and the symplectic form from  $W$ , restricted to  $V$ , is still alternating. Also for, all nonzero  $v \in V$  there exists  $w \in W$  such that  $\langle v, w \rangle \neq 0$  (because the form is nondegenerate on  $W$ ). But  $w \notin U$  because  $v$  pairs to zero with all elements of  $U$  so  $w \in V$  and the form is nondegenerate on  $V$ . Thus  $V$  is an  $(n - 2)$ -dimensional vector space with a symplectic form so by the inductive hypothesis  $V$  is isomorphic to the orthogonal direct sum of an integer number of copies of  $H$ .

But  $U$  is isomorphic to  $H$  by construction so  $W$  is the orthogonal direct sum of an integer number of copies of  $H$ .

## 2. The Cauchy–Frobenius Lemma

- (a) Let  $G$  be a finite group acting on a finite set  $X$ . If  $g \in G$ , let  $\text{Fix}(g)$  be the set of elements  $x \in X$  such that  $gx = x$ . Prove that the number of orbits of the action of  $G$  on  $X$  is equal to

$$\frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|.$$

First note that

$$\sum_{g \in G} |\text{Fix}(g)| = \sum_{x \in X} |\text{Stab}(x)|$$

as both are just the number of pairs  $(g, x)$  such that  $gx = x$ . Then

$$\begin{aligned} \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)| &= \sum_{x \in X} \frac{|\text{Stab}(x)|}{|G|} \\ &= \sum_{x \in X} \frac{1}{|\text{Orbit}(x)|} \\ &= \sum_{\{\text{Orbits}\}} 1 \\ &= \# \text{ of orbits} \end{aligned}$$

where the second equality is by the orbit stabiliser theorem.

- (b) How many different ways are there of colouring the vertices of a regular 11-gon using  $q$  different colours?

Let  $G = D_{11}$ , the dihedral group of symmetries of the regular 11-gon, act on  $X$ , the set of colourings of the 11 vertices NOT considering rotations or reflections to be the same. Then the number of orbits of the action of  $G$  on  $X$  will be the number of colourings considering two colourings that are rotations or reflections of each other to be the same.

So  $G = \langle r, s \mid r^{11} = s^2 = 1, srs = r^{10} \rangle$ ,  $|G| = 22$  and we consider the sum defined in part (a):

- (i)  $|\text{Fix}(1)| = q^{11}$  as the identity fixes any possible colouring.
- (ii)  $|\text{Fix}(r^i)| = q$  for  $i = 1, \dots, 10$  as if you rotate by  $i$  vertices the first and  $i$ th vertices must be the same colour and continuing this around we see (since 11 is prime) that all the vertices must be coloured the same. Thus there are  $q$  possible colourings, one for each colour.
- (iii)  $|\text{Fix}(r^i s)| = q^6$  for  $i = 0, \dots, 10$ . To see this recall that each of these elements is a reflection through one of the vertices. So if a colouring is to be fixed by this reflection there are 5 pairs of vertices which must be coloured the same and the vertex being reflected through is able to be coloured any colour. Thus there are 6 choices from the  $q$  colours.

So the number of different colourings is

$$\frac{1}{22}(q^{11} + 11q^6 + 10q).$$

- (c) How many different ways are there of colouring the faces of a cube with three different colours?

Let  $G$  be the group of symmetries of the cube. A symmetry of the cube is decided by where one face is sent to and it can be sent to any face so  $|G| = 6$ . We will think of the six

symmetries as the identity, 4 symmetries that rotate the sphere 90 degrees right, left, up and down and one that rotates it 180 degrees. Let  $X$  be the colourings of the six faces by three different colours.

Once again we use part (a):

- (i)  $|\text{Fix}(1)| = 3^6$  as the identity fixes any possible colouring.
- (ii)  $|\text{Fix}(90 \text{ degree rotation})| = 3^3$  as the four faces rotated must be one colour and the two faces left alone can be any colour.
- (iii)  $|\text{Fix}(180 \text{ degree rotation})| = 3^4$  as the opposite pairs in the direction of rotation must be the same colour and the two unchanged faces can be any colour.

So the number of possible colourings is

$$\frac{1}{6}(3^6 + 4 \cdot 3^3 + 3^4) = 153.$$

3. Groups of order  $p^3$ .

Let  $p$  be an odd prime. Determine the groups of order  $p^3$  as follows:

- (a) List the abelian groups of order
- $p^3$
- .

By the Chinese Remainder Theorem these are  $\mathbb{Z}/p^3$ ,  $\mathbb{Z}/p^2 \times \mathbb{Z}/p$  and  $\mathbb{Z}/p \times \mathbb{Z}/p \times \mathbb{Z}/p$ .

- (b) If
- $G$
- is any group with
- $G' \subseteq Z(G)$
- , prove that for all
- $x, y \in G$

$$(xy)^n = x^n y^n [y, x]^{n(n-1)/2}.$$

First note that  $[x, y] = xyx^{-1}y^{-1}$  so then  $[x, y]yx = xy$ . Thus  $yx = xy([x, y])^{-1} = xy[y, x]$ . We can use this to show by induction that under the assumptions of the question

$$(1) \quad yx^n = x^n y [y, x]^n$$

The  $n = 1$  case is already proved. For the inductive step

$$\begin{aligned} yx^n &= (yx^{n-1})x \\ &= x^{n-1}y[y, x]^{n-1}x \\ &= x^{n-1}yx[y, x]^{n-1} \\ &= x^{n-1}xy[y, x][y, x]^{n-1} \\ &= x^n y [y, x]^n \end{aligned}$$

where the second equality is by the inductive hypothesis and the third is using the fact that commutators are in the centre of the group.

Now we prove the desired equality, again by induction. The  $n = 1$  case is trivial. Then

$$\begin{aligned} (xy)^n &= (xy)(xy)^{n-1} \\ &= xyx^{n-1}y^{n-1}[y, x]^{(n-1)(n-2)/2} \\ &= xx^{n-1}y[y, x]^{n-1}y[y, x]^{(n-1)(n-2)/2} \\ &= x^n y^n [y, x]^{(n-1)(n-2)/2 + (n-1)} \\ &= x^n y^n [y, x]^{n(n-1)/2} \end{aligned}$$

where the second equality is by the inductive hypothesis and the third uses equation (1).

- (c) Suppose for the remainder of the problem that
- $G$
- is a non-abelian group of order
- $p^3$
- . Prove that
- $|Z(G)| = p$
- , that
- $G/Z(G) \cong (\mathbb{Z}/p)^2$
- , and that
- $G' = Z(G)$
- .

The centre,  $Z(G)$ , is a subgroup of  $G$  so has order dividing  $p^3$ . From class (and the class equation) we know that  $Z(G) \neq 1$ . Also  $Z(G) \neq G$  since  $G$  is not abelian and  $|Z(G)| \neq p^2$  for then  $G/Z(G)$  is cyclic (because size  $p$ ) so from homework  $G$  would be abelian. Therefore  $|Z(G)| = p$ .

Then  $|G/Z(G)| = p^2$  so is isomorphic to either  $\mathbb{Z}/p^2$  or  $\mathbb{Z}/p \times \mathbb{Z}/p$  but it cannot be the former because this would imply  $G$  abelian. Therefore  $G/Z(G) \cong (\mathbb{Z}/p)^2$ .

Finally  $G'$  is the minimal group such that  $G/G'$  is abelian. Thus  $G' \leq Z(G)$  but we know that  $G' \neq 1$  because  $G$  is non-abelian. So since  $Z(G)$  is cyclic and has no proper non-trivial subgroups we conclude that  $G' = Z(G)$ .

- (d) Show that the function
- $\phi: G \rightarrow G$
- defined by
- $\phi(x) = x^p$
- is a homomorphism whose image lies in
- $Z(G)$
- and check that
- $|\ker \phi| = p^2$
- or
- $p^3$
- .

To see  $\phi$  is homomorphism

$$\begin{aligned} \phi(xy) &= (xy)^p \\ &= x^p y^p [x, y]^{p(p-1)/2} \\ &= x^p y^p \\ &= \phi(x)\phi(y) \end{aligned}$$

where the third equality is because  $|G'| = p$  so the  $p$ th power of a commutator is the identity (and  $p$  is odd so  $(p-1)/2$  is an integer).

To see that  $\text{im } \phi \leq Z(G)$  note that for all  $y \in G$ , equation (1) gives

$$yx^p = x^p y [y, x]^{p(p-1)/2} = x^p y.$$

Therefore  $|\text{im } \phi|$  divides  $|Z(P)| = p$  so is 1 or  $p$ , so by the first isomorphism theorem

$$\frac{|G|}{|\ker \phi|} = |\text{im } \phi|,$$

we see that  $|\ker \phi| = p^2$  or  $p^3$ .

- (e) Suppose that  $|\ker \phi| = p^2$ . Prove that  $G$  must be isomorphic to a non-abelian semidirect product  $(\mathbb{Z}/p^2) \rtimes (\mathbb{Z}/p)$ . Check that there is exactly one of these.

The kernel of  $\phi$  is not the entire group  $G$ , so there must exist some element  $x \in G$  of order greater than  $p$ . But it cannot be of order  $p^3$  because then  $G$  would be abelian. Thus  $x$  is of order  $p^2$  and  $H = \langle x \rangle \cong \mathbb{Z}/p^2$  is a normal subgroup of  $G$  because it is index  $p$  and  $p$  is the smallest prime dividing the order of the group.

Since  $x \notin \ker \phi$  and  $|\ker \phi| = |H|$  there exists a nontrivial  $y \in \ker \phi$  such that if  $y \in H$  then  $y = 1$ . Then  $K = \langle y \rangle \cong \mathbb{Z}/p$  and we can check that  $H \cap K = \{1\}$ : If  $x^a = y^b$  then  $y = (x^a)^{b^{-1}}$  (taking inverse of  $b$  modulo  $p$ ) so  $ab^{-1} = 0$  and  $a = 0$ .

Then  $HK = G$  so  $G = H \rtimes K \cong (\mathbb{Z}/p^2) \rtimes_{\psi} (\mathbb{Z}/p)$ . This is nonabelian so must have a nontrivial map  $\psi$ . We check that there is only one such product: Possible maps

$$\psi: \mathbb{Z}/p \rightarrow \text{Aut}(\mathbb{Z}/p^2) \cong \mathbb{Z}/p(p-1)$$

must send the  $p-1$  elements of order  $p$  to the  $p-1$  elements of order  $p$  and thus the image of cyclic  $K$  under any two nontrivial maps must be the same. So by Corollary 3 of the semidirect products handout any two nontrivial maps  $\psi$  would give rise to isomorphic semidirect products.

- (f) Suppose that  $|\ker \phi| = p^3$ . Prove that  $G$  must be isomorphic to a non-abelian semidirect product  $(\mathbb{Z}/p \times \mathbb{Z}/p) \rtimes (\mathbb{Z}/p)$ . Check that there is exactly one of these.

The kernel of  $\phi$  is the whole group so every non-identity element has order  $p$ . Now  $p$ -groups have subgroups of all possible orders so there exists  $H \leq P$  with  $|H| = p^2$ . Then  $H \triangleleft P$  because index  $p$  and  $H \cong \mathbb{Z}/p \times \mathbb{Z}/p$  because groups of order  $p^2$  are abelian and there are no elements of order  $p^2$  in  $P$ .

Now take  $z \notin H$  and consider  $K = \langle z \rangle \cong \mathbb{Z}/p$ . If  $z^a \in H$  with  $a \neq 0$  then  $(z^a)^{a^{-1}} = z \in H$  which is a contradiction so  $H \cap K = 1$ . Thus  $HK = G$  and  $G = H \rtimes K \cong (\mathbb{Z}/p \times \mathbb{Z}/p) \rtimes_{\psi} (\mathbb{Z}/p)$  for some nontrivial map  $\psi$ .

We now check that there is only one such product: Possible maps

$$\psi: \mathbb{Z}/p \rightarrow \text{Aut}(\mathbb{Z}/p \times \mathbb{Z}/p) \cong \text{GL}(2, \mathbb{F}_p)$$

send the generator 1 to an element of order  $p$ . From the semidirect products handout if  $\psi_1$  and  $\psi_2$  were two nontrivial maps then  $\psi_1(K)$  and  $\psi_2(K)$  would be two subgroups of order  $p$  in  $\text{GL}(2, \mathbb{F}_p)$  so would be conjugate (Proposition 5) so then the two semidirect products would be isomorphic (Corollary 3).

- (g) Conclude that there are exactly two non-isomorphic non-abelian groups of order  $p^3$ . Prove that these two groups can be realised as the matrix groups

$$G_1 = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a, b \in \mathbb{Z}/p^2, a \equiv 1 \pmod{p} \right\}$$

and

$$G_2 = \left\{ \left( \begin{array}{ccc} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{array} \right) \in \text{GL}(3, \mathbb{F}_p) \right\}.$$

Which is which?

From part (c) we know that either  $|\ker(\phi)| = p^2$  or  $|\ker(\phi)| = p^3$  and then parts (e) and (f) tell us there is exactly one group of order  $p^3$  in each case. We give two groups of order  $p^3$ , check that they are non-abelian and that they are not isomorphic to each other. This shows that there are exactly two non-abelian groups of order  $p^3$ .

First we show that  $G_1 \leq \text{GL}(2, \mathbb{F}_{p^2})$ . If

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} \in G_1$$

then

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} ac & ad+b \\ 0 & 1 \end{pmatrix} \in G_1$$

because if  $a \equiv 1 \pmod{p}$  and  $c \equiv 1 \pmod{p}$  then  $ac \equiv 1 \pmod{p}$ .

Also

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} a^{p-1} & -ba^{p-1} \\ 0 & 1 \end{pmatrix} \in G_1$$

because  $a \equiv 1 \pmod{p}$  implies  $a^{p-1} \equiv 1 \pmod{p}$ .

To see  $|G_1| = p^3$  note that there are  $p^2$  choices for  $b$ , and  $p$  choices  $(1, p+1, \dots, (p-1)p+1)$  for  $a$  and that all of these choices give distinct matrices with non-zero determinant. The group  $G_1$  is not abelian because

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} p+1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} p+1 & 2 \\ 0 & 1 \end{pmatrix}$$

does not equal

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

Next we show  $G_2 \leq \text{GL}(3, \mathbb{F}_p)$ . If

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} \in G_2$$

then

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+d & e+af+b \\ 0 & 1 & f+c \\ 0 & 0 & 1 \end{pmatrix} \in G_2$$

and

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix} \in G_2.$$

Now there are  $p$  choices for each of  $a$ ,  $b$  and  $c$  and all of these choices lead to distinct matrices with non-zero determinant so  $|G_2| = p^3$ . To see that  $G_2$  is non-abelian we find that

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$$

is not equal to

$$\begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 2 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}.$$

To see these two groups are not isomorphic we show that every element of  $G_2$  has order dividing  $p$ . In fact, we show by induction that for  $n$  odd

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & na & nb + \frac{n(n-1)}{2}ac \\ 0 & 1 & nc \\ 0 & 0 & 1 \end{pmatrix}.$$

The  $n = 1$  case is trivial. For the inductive case

$$\begin{aligned} \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^n &= \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^{n-2} \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^2 \\ &= \begin{pmatrix} 1 & (n-2)a & (n-2)b + \frac{(n-2)(n-3)}{2}ac \\ 0 & 1 & (n-2)c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2a & 2b + ac \\ 0 & 1 & 2c \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2a + (n-2)a & 2b + ac + (n-2)ac + (n-2)b + \frac{(n-2)(n-3)}{2}ac \\ 0 & 1 & 2c + (n-2)c \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & na & nb + \frac{n(n-1)}{2}ac \\ 0 & 1 & nc \\ 0 & 0 & 1 \end{pmatrix}. \end{aligned}$$

So

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^p = \begin{pmatrix} 1 & pa & pb + \frac{p(p-1)}{2}ac \\ 0 & 1 & pc \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

However, in  $G_1$ ,

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$$

so this matrix has order  $p^2$ . Thus  $G_1 \not\cong G_2$ . We also see that since  $(1, 0) \in \mathbb{Z}/p^2 \rtimes \mathbb{Z}/p$  has order  $p^2$

$$G_1 \cong (\mathbb{Z}/p^2) \rtimes (\mathbb{Z}/p) \text{ and } G_2 \cong (\mathbb{Z}/p \times \mathbb{Z}/p) \rtimes (\mathbb{Z}/p).$$

(h) Prove that these two groups have presentations

$$T_1 = \langle x, y \mid x^{p^2} = y^p = 1, yxy^{-1} = x^{1+p} \rangle$$

and

$$T_2 = \langle x, y, z \mid x^p = y^p = z^p = 1, [x, z] = [y, z] = 1, [x, y] = z \rangle.$$

Which is which?

We provide a map of the generators of  $T_1$  to  $G_1$  and  $T_2$  to  $G_2$  and check that the elements mapped to satisfy the relations. Then Van Dyck's Theorem tells us that we have a surjective homomorphism from the presentations to the matrix groups. Then by seeing that the number of elements in each presentation is at most  $p^3$  we conclude that the homomorphisms are isomorphisms.

Map the generators of  $T_1$  to  $G_1$  by

$$x \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } y \mapsto \begin{pmatrix} p+1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Then

$$x^{p^2} = \begin{pmatrix} 1 & p^2 \\ 0 & 1 \end{pmatrix} = I,$$

$$y^p = \begin{pmatrix} (p+1)^p & 0 \\ 0 & 1 \end{pmatrix} = I,$$

and

$$\begin{aligned} yxy^{-1} &= \begin{pmatrix} p+1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} (p+1)^{p-1} & 0 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} p+1 & p+1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} (p+1)^{p-1} & 0 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & p+1 \\ 0 & 1 \end{pmatrix} \\ &= x^{p+1}. \end{aligned}$$

So we have a surjective homomorphism  $T_1 \rightarrow G_1$ . Now in  $T_1$ ,  $x^{-1} = x^{p^2-1}$  and  $y^{-1} = y^{p-1}$  so we can use the relation  $yx = x^{1+p}y$  to write any element in the form  $x^a y^b$  and then use  $x^{p^2} = 1$  and  $y^p = 1$  to write the element as  $x^a y^b$  with  $a = 0, 1, \dots, p^2$  and  $b = 0, 1, \dots, p$ . Thus there are at most  $p^3$  elements in  $T_1$ , which maps surjectively onto a group of order  $p^3$ . Therefore  $T_1 \cong G_1 \cong (\mathbb{Z}/p^2) \rtimes (\mathbb{Z}/p)$ .

Now map the generators of  $T_2$  to  $G_2$  by

$$x \mapsto \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, y \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } z \mapsto \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Then

$$x^p = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^p = \begin{pmatrix} 1 & p & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = I$$

and similarly  $y^p = I$  and  $z^p = I$ .

Next,

$$\begin{aligned} [x, y] &= xyx^{-1}y^{-1} \\ &= \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = z. \end{aligned}$$

Also,

$$\begin{aligned}
[x, z] &= xzx^{-1}z^{-1} \\
&= \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = I.
\end{aligned}$$

Finally,

$$\begin{aligned}
[y, z] &= yzy^{-1}z^{-1} \\
&= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = I.
\end{aligned}$$

So we have a surjective homomorphism  $T_2 \rightarrow G_2$ . Now in  $T_2$  we know that  $x^{-1} = x^{p-1}$  and similarly for  $y, z$ . Thus we can write any element as a product of positive powers of  $x, y, z$  and then use the relations  $[x, z] = [y, x] = 1$  and  $[x, y] = z$  to collect all the powers of  $x$  together at the cost of introducing  $z$ 's. Then we can collect the  $y$ 's together without producing any more  $x$ 's. Thus any element of  $T_2$  can be written in the form  $x^a y^b z^c$  and then using the fact that these elements are of order  $p$  we can take  $a, b, c$  all to be one of  $0, 1, \dots, p-1$ . So there are at most  $p^3$  elements of  $T_2$ . But  $T_2$  maps surjectively onto a group of order  $p^3$  so this map must be an isomorphism and  $T_2 \cong G_2 \cong (\mathbb{Z}/p \times \mathbb{Z}/p) \rtimes (\mathbb{Z}/p)$ .

## 4. Burnside's basis theorem.

If  $G$  is a group, then a proper subgroup  $M < G$  is *maximal* if there is no group lying strictly between  $M$  and  $G$ . The *Frattini subgroup*  $\Phi(G)$  is the intersection of all the maximal subgroups of  $G$ .

Let  $P$  be a group of order  $p^a$  with  $p$  a prime.

- (a) If  $H$  is a proper subgroup of  $P$ , show that  $H$  is a proper subgroup of  $N_P(H)$ .

Note that  $hHh^{-1} = H$  for all  $h \in H$  so  $H$  is a subgroup of  $N_P(H)$ . To prove it is a proper subgroup we use induction on  $a$ . For  $a = 1$  or  $2$ ,  $P$  is abelian so  $N_P(H) = G$  and the statement is trivial. For the inductive step we use two cases:

- (i) If  $Z(P) \not\leq H$ . First note that if  $z \in Z(P)$  then  $zHz^{-1} = H$  so  $Z(P) \leq N_P(H)$ . Thus if  $Z(P) \not\leq H$  then there are some elements of  $N_P(H)$  not in  $H$  so  $H$  is a proper subgroup of  $N_P(H)$ .

- (ii) If  $Z(P) \leq H$ . Since  $P$  is a  $p$ -group,  $|Z(P)| > 1$  so  $|P/Z(P)| < p^a$ . Thus by our inductive hypothesis, and the fact that  $H$  properly contained in  $P$  means that  $H/Z(P)$  is properly contained in  $P/Z(P)$ , we know that  $H/Z(P)$  is properly contained in  $N_{P/Z(P)}(H/Z(P))$ . But  $N_{P/Z(P)}(H/Z(P)) = N_P(H)/Z(P)$ : to see this use the correspondence theorem or simply notice that  $xZ(P) \in N_{P/Z(P)}(H/Z(P))$  iff  $(xZ(P))(hZ(P))(xZ(P))^{-1} \in H/Z(P)$  for all  $h \in H$  iff  $xhx^{-1} \in H$  for all  $h \in H$  iff  $x \in N_P(H)$  iff  $xZ(P) \in N_P(H)/Z(P)$ . So  $H/Z(P)$  is properly contained in  $N_P(H)/Z(P)$  which implies that  $H$  is properly contained in  $N_P(H)$ .

- (b) If  $H$  is a maximal subgroup of  $P$ , prove that  $H \triangleleft P$  and  $[P : H] = p$ .

If  $H$  is a maximal subgroup of  $P$  then it is proper so by part (a) we have that  $H$  is properly contained in  $N_P(H)$ . But  $H$  is maximal so  $N_P(H) = G$  and therefore  $H \triangleleft P$ .

Now if  $[P : H] = p^3$  then  $H = 1$  and is clearly not maximal. If  $[P : H] = p^2$  then  $|H| = p$ . Then  $|P/H| = p^2$  so this quotient contains a subgroup of order  $p$ , call it  $K$ . If  $\phi: P \rightarrow P/H$  is the quotient map let  $H' = \phi^{-1}(K)$ . Then  $H \leq H'$  and  $\phi|_{H'}: H' \rightarrow K$  is surjective so  $|H'| = |H||K| = p^2$  by the first isomorphism theorem. Therefore  $H$  is not maximal.

So since  $H$  is a proper subgroup of a group of order  $p^3$  we must have  $[P : H] = p$ .

- (c) Show that  $P/\Phi(P) \cong (\mathbb{Z}/p)^r$  for some integer  $r$ .

First assume that  $P$  is abelian. Then  $P \cong \mathbb{Z}/p^{a_1} \times \cdots \times \mathbb{Z}/p^{a_n}$  with  $a_i \geq 1$ . Now maximal subgroups of  $P$  are of the form  $\mathbb{Z}/p^{a_1} \times \cdots \times \mathbb{Z}/p^{a_{i-1}} \times \cdots \times \mathbb{Z}/p^{a_n}$  for some  $i$  and groups of this form are maximal so  $\Phi(P) = \mathbb{Z}/p^{a_1-1} \times \cdots \times \mathbb{Z}/p^{a_n-1}$  and  $P/\Phi(P) = \mathbb{Z}/p \times \cdots \times \mathbb{Z}/p$ . If  $P$  is non abelian then we can mod out by its commutator subgroup so the above argument applied to  $P/P'$  gives us  $(P/P')/\Phi(P/P') \cong (\mathbb{Z}/p)^r$ . Then

$$\frac{P}{\Phi(P)} \cong \frac{P/P'}{\Phi(P)/P'} \cong \frac{P/P'}{\Phi(P/P')} \cong (\mathbb{Z}/p)^r.$$

The first isomorphism is by the third isomorphism theorem and the second is noting that  $\Phi(P)/P' = \Phi(P/P')$ . This equality follows from noting that maximal subgroups of  $P$  contain  $P'$  (because  $P'$  is the minimal group such that  $P/P'$  is abelian) so the maximal subgroups of  $P$  are in one-to-one correspondence with the maximal subgroups of  $P/P'$ . So if  $H_i$  are the maximal subgroups of  $P$  we have

$$\Phi(P)/P' = (\cap H_i)/P' = \cap (H_i/P') = \Phi(P/P').$$

- (d) Prove that  $P = \langle x_1, \dots, x_s \rangle$  iff  $x_1\Phi(P), \dots, x_s\Phi(P)$  generate  $P/\Phi(P)$

First we prove (as suggested) that if  $H \leq G$  then  $\Phi(G)H = G$  implies  $H = G$ .

To see this, if  $H \neq G$  then  $H$  is contained in some maximal subgroup of  $G$ . Then  $\Phi(G)$  and  $H$  are both contained in this maximal subgroup so  $\Phi(G)H$  is also and is not equal to  $G$ . Therefore if  $\Phi(G)H = G$  we must be in the case  $H = G$ .

Now, if  $P$  is generated by  $x_1, \dots, x_s$  then every element of  $P/\Phi(P)$  can be written as  $x\Phi(P)$  for some  $x \in P$ . Then  $x$  can be written as a product of elements of  $x_1, \dots, x_s$  and their inverses so  $x\Phi(P)$  can be written as a product of  $x_1\Phi(P), \dots, x_s\Phi(P)$  and their inverses. That is,  $x_1\Phi(P), \dots, x_s\Phi(P)$  generate  $P/\Phi(P)$ .

If  $x_1\Phi(P), \dots, x_s\Phi(P)$  generate  $P/\Phi(P)$  consider  $H = \langle x_1, \dots, x_s \rangle \leq P$ . Now for all  $x \in P$ ,  $x\Phi(P) \in P/\Phi(P)$  so  $x\Phi(P) = h\Phi(P)$  for some  $h \in H$ , therefore  $x = hy$  for some  $y \in \Phi(P)$ . So  $G \leq \Phi(P)H$ , therefore  $G = \Phi(P)H$  and by the fact proved above,  $G = H$ ; that is  $G = \langle x_1, \dots, x_s \rangle$ .

(e) Verify Burnside's basis theorem ( $r$  is the size of the smallest generating set of  $P$ ) directly for each of the five groups of order  $p^3$ .

- (i) If  $P = \mathbb{Z}/p^3 = \langle x \mid x^{p^3} = 1 \rangle$  then  $x^p$  generates the unique subgroup of order  $p^2$  so  $\Phi(P) = \langle x^p \rangle$  so  $P/\Phi(P) = \langle x\Phi(P) \rangle \cong \mathbb{Z}/p$ . So  $r = 1$  which agrees with  $P$  being generated by one element.
- (ii) If  $P = \mathbb{Z}/p^2 \times \mathbb{Z}/p = \langle x, y \mid x^{p^2} = y^p = 1 \rangle$  then  $\langle x \rangle$  and  $\langle x^p, y \rangle$  are two maximal subgroups so  $\Phi(P) \leq \langle x \rangle \cap \langle x^p, y \rangle = \langle x^p \rangle$ . Also any maximal subgroup must contain a nontrivial element of  $\langle x \rangle$  (because  $\langle y \rangle$  can only contribute  $p$  elements) so must contain its only proper nontrivial subgroup,  $\langle x^p \rangle$ . So  $\Phi(P) = \langle x^p \rangle$  which gives  $P/\Phi(P) = \langle x\Phi(P), y\Phi(P) \rangle \cong \mathbb{Z}/p \times \mathbb{Z}/p$ . So  $r = 2$  and  $P$  is generated by two elements (it is not cyclic so cannot be generated by one).
- (iii) If  $P = \mathbb{Z}/p \times \mathbb{Z}/p \times \mathbb{Z}/p = \langle x, y, z \mid x^p = y^p = z^p = 1 \rangle$  then  $\Phi(P) \leq \langle x, y \rangle \cap \langle x, z \rangle \cap \langle y, z \rangle = 1$ . Therefore  $P/\Phi(P) \cong P \cong \mathbb{Z}/p \times \mathbb{Z}/p \times \mathbb{Z}/p$ . So  $r = 3$  and this is the minimum number of generators needed to describe  $P$  (every nonidentity element of  $P$  has order  $p$  and  $P$  is abelian so two generators would give at most  $p^2$  elements).
- (iv) If  $P = \mathbb{Z}/p^2 \rtimes \mathbb{Z}/p = \langle x, y \mid x^{p^2} = y^p = 1, yxy^{-1} = x^{1+p} \rangle$  then  $\Phi(P) \leq \langle x \rangle \cap \langle x^p, y \rangle = \langle x^p \rangle$  and as in (ii) this implies that  $\Phi(P) = \langle x^p \rangle$ . Therefore  $P/\Phi(P) = \langle x\Phi(P), y\Phi(P) \rangle \cong \mathbb{Z}/p \times \mathbb{Z}/p$ . Note that  $yxy^{-1}\Phi(P) = x^{1+p}\Phi(P) = x\Phi(P)$  so it is indeed the direct product. So  $r = 2$  agrees with the fact that we know  $P$  is generated by two elements (and is not cyclic).
- (v) If  $P = (\mathbb{Z}/p \times \mathbb{Z}/p) \rtimes \mathbb{Z}/p = \langle x, y, z \mid x^p = y^p = z^p = 1, [x, z] = [y, z] = 1, [x, y] = z \rangle$  then since  $x, z$  commute and  $y, z$  commute we have maximal subgroups  $\langle x, z \rangle$  and  $\langle y, z \rangle$ . Now every nonidentity element of  $P$  has order  $p$  (shown in question 3) so a maximal subgroup (of order  $p^2$ ) must contain one non-identity element from at least two of  $\langle x \rangle, \langle y \rangle$  or  $\langle z \rangle$ . These groups are cyclic so  $H$  contains at least two of  $x, y, z$ . Either  $z \in H$  or  $x, y \in H$  but then  $z = [x, y] \in H$ . So  $\langle z \rangle \leq \Phi(P) \leq \langle x, z \rangle \cap \langle y, z \rangle = \langle z \rangle$  which gives us  $\Phi(P) = \langle z \rangle$ . Then  $P/\Phi(P) = \langle x\Phi(P), y\Phi(P) \rangle \cong \mathbb{Z}/p \times \mathbb{Z}/p$  because  $[x, y] \in \Phi(P)$ . So  $r = 2$  which agrees with the fact that  $P$  can have a generating set  $\{x, y\}$  of size 2 (because  $z = [x, y]$ ) and is not cyclic.