Exercise: How many distinct ways are there of marking 3 circles on a triangular board of 10 circles, *up to symmetry*?

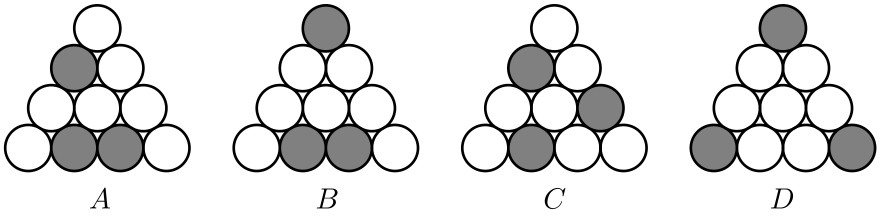


Figure 1

For example, pattern A in Figure 1 is totally asymetric, so there are a total of 6 patterns which look like A under the action of the triangle group. We only want to count such a pattern once.

Pattern B has a flip symmetry, so there are two other patterns which look like it, obtained by rotation. Pattern C has rotational symmetry, so there is one other pattern which looks like it, obtained by flipping. Pattern D is totally symmetric. We only want to count each of these patterns once.

Let x_A, x_B, x_C, x_D be the number of patterns of symmetry types A, B, C, and D, counted up to symmetry. It is hard to compute these quantities directly; it is easier to count patterns having *at least* a certain kind of symmetry, without worrying about matching up patterns which are really the same. We then figure out the coefficients of x_A, x_B, x_C, x_D in these easier counts, in order to solve for $x_A + x_B + x_C + x_D$.

We know that there are three *conjugate* flavors of flip symmetry, corresponding to the three possible axis of flipping. It is enough to only consider one of these flavors, only counting patterns having at least, say, vertical axis flip symmetry. Every pattern with flip symmetry has one representative with vertical axis flip symmetry, so we will count all such patterns once.

There is only one flavor of rotational symmetry, because rotations are a *normal* subgroup of the triangle group. Every pattern with rotational symmetry has two representatives, one the flip of the other.

[**1**] Let y_A be the number of ways of marking 3 circles on our board, if we don't worry about symmetry. Show that $y_A = \frac{10 \cdot 9 \cdot 8}{3 \cdot 2 \cdot 1} = 120$.

(Hint: There are 10 choices for where to mark first, and then 9 choices left for where to mark second, and then 8 choices left for where to mark third. However, we don't care in what order we mark a given pattern. How many times does $10 \cdot 9 \cdot 8$ count each pattern?)

[**2**] Let y_B be the number of ways of marking 3 circles on our board, so the resulting pattern is symmetric with respect to flipping across the vertical axis. To get an easy formula, don't worry about also counting patterns which are even more symmetric. Show that $y_B = 2 \cdot 4$.

[3] Let y_C be the number of ways of marking 3 circles on our board, so the resulting pattern is rotationally symmetric. Don't worry if two patterns in your count are the same after flipping, and don't worry about counting patterns which are even more symmetric. Show that $y_C = 3$.

[4] Let y_D be the total number of ways of marking 3 circles on our board, so the resulting pattern is completely symmetric. Show that $y_D = 1$.

[5] Now consider two patterns to be the same if they are the same up to symmetry. Figure out the coefficients of the linear equation

$$y_A \quad = \quad a\,x_A \;+\; b\,x_B \;+\; c\,x_C \;+\; d\,x_D.$$

In other words, how many times does y_A count a pattern which is totally asymetric, like A? This is the coefficient a. How many times do patterns of types B, C, and D get counted? These are the coefficients b, c, and d.

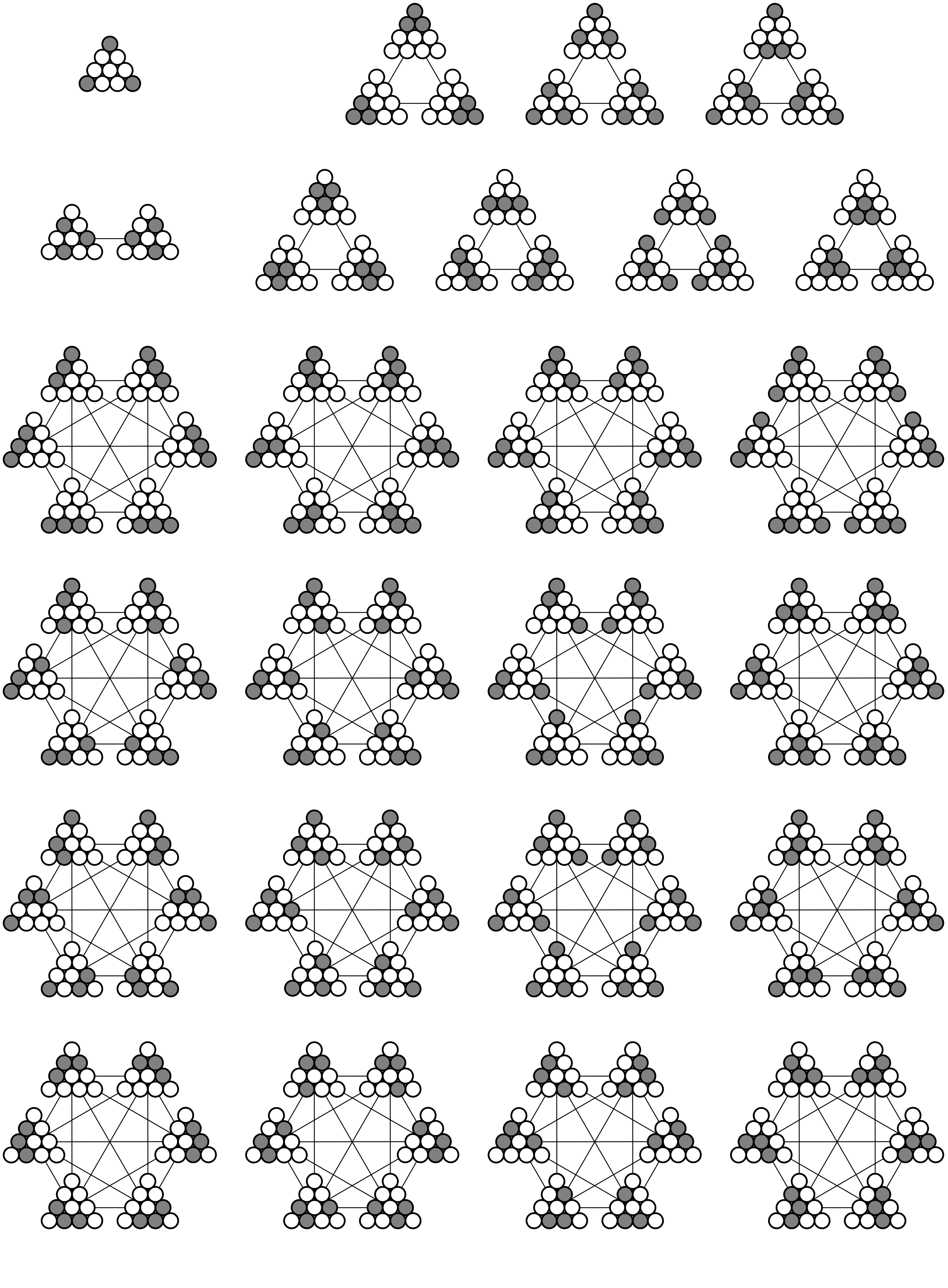
[6] Figure out similar linear equations for y_B, y_C, and y_D. Solve this system of equations to find x_A, x_B, x_C, and x_D. The sum $x_A + x_B + x_C + x_D$ is the number of distinct ways there are of marking 3 circles on a triangular board of 10 circles, up to symmetry.

This is a tricky problem, until you get the hang of this method. If you can't get your system of equations to work out nicely, list all the possibilities of types B, C, and D by hand, and substitute these values into your equations to see where you went wrong.

Notice that your reasoning in [5] and [6] has nothing to do with the board size, or the number of marks; it only depends on the structure of the triangle group. We can use the above system of linear equations to solve for $x_A + x_B + x_C + x_D$ in terms of y_A, y_B, y_C, and y_D. This final equation is useful for other size problems; we only have to recompute y_A, y_B, y_C, and y_D. Try it!

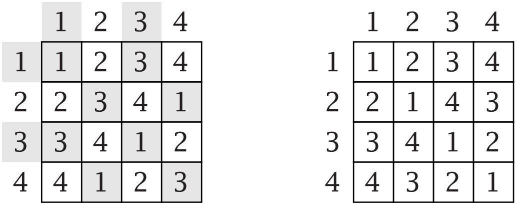
The truly obsessed may want to play with the group of 8 symmetries of the square, and redo this entire problem for marking square boards. Reviewing both problems, can you see a pattern to the coefficients you get in the final equations?

The slickest way of stating this counting technique is known as Polya enumeration.



First homework problems

Dave Bayer, Modern Algebra, September 9, 1998



	1	2	3	4
1	1	2	3	4
2	2	3	4	1
3	3	4	1	2
4	4	1	2	3

	1	2	3	4
1	1	2	3	4
2	2	1	4	3
3	3	4	1	2
4	4	3	2	1

Figure 1

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	3	4	5	6	1
3	3	4	5	6	1	2
4	4	5	6	1	2	3
5	5	6	1	2	3	4
6	6	1	2	3	4	5

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	3	1	6	4	5
3	3	1	2	5	6	4
4	4	5	6	1	2	3
5	5	6	4	3	1	2
6	6	4	5	2	3	1

Figure 2

[**1**] Find all subgroups of the groups whose multiplication tables are shown in Figures 1 and 2.

[**2**] For the group on the left in Figure 1, a *quotient group* has been colored in: The multiplication rule for *grey* and *white* is independent of which elements are chosen to represent the grey and white "teams". Notice that the grey "team" is one of the subgroups you found in problem 1, now playing the role of the identity in the quotient group.

Find all quotient groups of the groups whose multiplication tables are shown in Figures 1 and 2. In every case, does a subgroup play the role of the identity in the quotient? Does every subgroup you found in problem 1 make an appearance in this problem?

[**3**] Write down the multiplication table for the group of pairs of integers under addition modulo (2,3)

$$\mathbb{Z}_2 \times \mathbb{Z}_3 \quad = \quad \{\ (0,0),\ (0,1),\ (0,2),\ (1,0),\ (1,1),\ (1,2)\ \}$$

where $(a,b)+(c,d) = (a+c \bmod 2,\ b+d \bmod 3)$. Does the pattern of its multiplication table look familiar? You may need to rearrange and relabel the rows and columns.

[**4**] Write down the multiplication table for the group of permutations on three elements

$$S_3 \quad = \quad \{\ (\,),\ (123),\ (132),\ (12),\ (13),\ (23)\ \}\,.$$

Does the pattern of its multiplication table look familiar? You may need to rearrange and relabel the rows and columns.

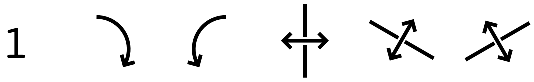


Figure 3

[**5**] There are six ways to rotate, flip, or leave alone a triangle, so each corner goes to some corner. Make up a visual notation for these six operations, such as that given in Figure 3. Write down the multiplication table for this group of symmetries of a triangle. Does the pattern of its multiplication table look familiar? You may need to rearrange and relabel the rows and columns.

[**6**] Let G be the group of all 2×2 matrices whose entries are integers mod 2, and whose determinants are nonzero. How many elements does G have? Write down the multiplication table for this group. Does the pattern of its multiplication table look familiar? You may need to rearrange and relabel the rows and columns.

[**7**] There are six ways to rotate, flip, or leave alone a triangle, so each corner goes to some corner. Make up a visual notation for these six operations. Write down the multiplication table for this group of symmetries of a square.

[**8**] Let

$$G \quad = \quad \{\, 1,\ -1,\ \mathbf{i},\ -\mathbf{i},\ \mathbf{j},\ -\mathbf{j}\ ,\ \mathbf{k},\ -\mathbf{k}\}\,.$$

be a group under multiplication ×, where **i**, **j**, **k** obey the familiar cross-product rules from multivariate calculus

$$\mathbf{i}\times\mathbf{j}=\mathbf{k},\ \ \mathbf{j}\times\mathbf{k}=\mathbf{i},\ \ \mathbf{k}\times\mathbf{i}=\mathbf{j},\ \ \mathbf{j}\times\mathbf{i}=-\mathbf{k},\ \ \mathbf{k}\times\mathbf{j}=-\mathbf{i},\ \ \mathbf{i}\times\mathbf{k}=-\mathbf{j}.$$

Write down the multiplication table for this group. Is this the same group as in problem 7?

Second homework problems

Dave Bayer, Modern Algebra, September 30, 1998

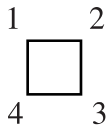


Figure 1

Problems 1 through 5 all concern the group G of symmetries of a square.

[**1**] The group G of symmetries of the square has 8 elements: the identity, 3 rotations, and 4 flips. G can be generated by two elements: a quarter-turn a, and a flip b. By numbering the square as shown in Figure 1, express the 8 elements of G as permutations on $\{1,2,3,4\}$. This expresses G as a subgroup of the group S_4 of all permutations on $\{1,2,3,4\}$. What permutations represent your choices of a and b?

[**2**] In terms of generators and relations, G can be written as the group

$$G \quad = \quad \langle\, a,\, b \mid a^4 = b^2 = 1, \;\; b\,a = a^m\, b \,\rangle$$

for some choice of m. What is m? Listing the elements of G in the form

$$1,\ a,\ a^2,\ a^3,\ b,\ a\,b,\ a^2\,b,\ a^3\,b,$$

describe each of these elements both as symmetries of the square, and as permutations in S_4.

[**3**] Show that S_4 can be generated by the two permutations $c = (1\ 2)$ and $d = (1\ 2\ 3\ 4)$. How would you demonstrate this to a high school student, using props but no notation?

[**4**] Decide whether or not G is a normal subgroup of S_4, using the criterion

$$G \subset S_4 \quad \text{is normal} \quad \Longleftrightarrow \quad g\,G\,g^{-1} \;=\; G \quad \text{for all} \quad g \in S_4.$$

Show that it is enough to check that $g\,h\,g^{-1} \in G$ for each generator g of S_4 and each generator h of G. Apply this to the generators c, d of S_4 and a, b of G which you found above, checking

$$c\,a\,c^{-1} \in G\,? \qquad c\,b\,c^{-1} \in G\,? \qquad d\,a\,d^{-1} \in G\,? \qquad d\,b\,d^{-1} \in G\,?$$

[**5**] Decide whether or not the subgroup $H = \{1,\, a,\, a^2,\, a^3\} \subset G$ generated by a is normal in G, using the same method. Repeat, for the subgroup $H = \{1,\, b\} \subset G$ generated by b.

The remaining problems are independent of each other.

[6] Let the group G be given in terms of generators and relations as

$$G \quad = \quad \langle\, a,\, b,\, c \mid a\,b\,c \,=\, a\,c\,b \,=\, 1 \,\rangle.$$

How many distinct elements does G have? Your answer may surprise you. Can you give a simpler presentation of G, perhaps using fewer generators? Do you recognize G?

[7] Let the group G be given in terms of generators and relations as

$$G \quad = \quad \langle\, a,\, b \mid a^3 = b^3 = 1,\;\; b\,a = a^2\,b \,\rangle.$$

How many distinct elements does G have? Your answer may surprise you. Can you give a simpler presentation of G, perhaps using fewer generators?

[8] (challenging) Let p and q be prime numbers. For which integers m, $1 \leq m < p$, does the presentation

$$G \quad = \quad \langle\, a,\, b \mid a^p = b^q = 1,\;\; b\,a = a^m\,b \,\rangle.$$

describe a group with $p\,q$ distinct elements? For these values of m, when is the subgroup generated by a normal? When is the subgroup generated by b normal?

Practice problems for first midterm

Dave Bayer, Modern Algebra, September 29, 1997

[**1**] Give an example of a group G and a subgroup H, where
(a) H is normal. What is the quotient group G/H?
(b) H is not normal. Show that H is not normal, by finding an element $g \in G$ with the property that the cosets $gH \neq Hg$.

[**2**] Let G be the group $\mathbb{Z}_4 \times \mathbb{Z}_4$. Let H be the subgroup of G generated by the element $(1,1)$.
(a) What is the order of H?
(b) List the cosets of H in G. (Since G is abelian, left and right cosets are the same.)

[**3**] Let G be the group of 2 by 2 matrices whose entries are integers mod 7, and whose determinant is nonzero mod 7. Let H be the subset of G consisting of all matrices whose determinant is 1 mod 7.
(a) How many elements are there in G and in H?
(b) Show that H is a normal subgroup of G.
(c) What familiar group is isomorphic to the quotient group G/H?

[**4**] The *center* $Z(G)$ of a group G is the set of all elements of G which commute with every element of G:

$$Z(G) \quad = \quad \{\ g \in G \mid gh = hg \text{ for every } h \in G\ \}.$$

(a) Show that $Z(G)$ is a subgroup of G.
(b) Show that $Z(G)$ is in fact a normal subgroup of G.

[**5**] The *normalizer* $N(H)$ of a subgroup H of a group G is the set of all elements of G whose left and right H-cosets are the same:

$$N(H) \quad = \quad \{\ g \in G \mid gH = Hg\ \}.$$

(a) Show that $N(H)$ is a subgroup of G.
(b) Show that H is a normal subgroup of $N(H)$.

[**6**] Consider the two groups $G = \mathbb{Z}_2 \times \mathbb{Z}_5$ and $H = \mathbb{Z}_{10}$.
(a) Describe each of these groups using generators and relations.
(b) Find an isomorphism between G and H.

[7] Draw the Cayley graph of the group of order 6 defined using generators and relations by

$$G \quad = \quad \langle\, a, b \mid a^3 = 1,\ b^2 = 1,\ ba = a^2 b \,\rangle.$$

What familiar group is isomorphic to G? Give an isomorphism.

[8] Draw the Cayley graph of the group of order 9 defined using generators and relations by

$$G \quad = \quad \langle\, a, b \mid a^3 = 1,\ b^3 = 1,\ ba = ab \,\rangle.$$

What familiar group is isomorphic to G? Give an isomorphism.

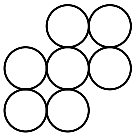


Figure 1

[9] How many ways are there of marking some (or none, or all) of the cells in Figure 1, up to symmetry? Consider two patterns to be the same if one can be obtained from the other by rotating or flipping. Use Burnside's formula

$$(\text{\# of patterns up to symmetry}) \quad = \quad \frac{1}{|G|} \sum_{g \in G} (\text{\# of patterns fixed by } g),$$

where G is the group of symmetries of this configuration of cells.

First Midterm

Dave Bayer, Modern Algebra, October 6, 1997

[**1**] Give an example of a group G and a subgroup H, where
(a) H is normal. What is the quotient group G/H?
(b) H is not normal. Show that H is not normal, by finding an element $g \in G$ with the property that the cosets $gH \neq Hg$.

[**2**] Let G be the group of 2 by 2 matrices whose entries are integers mod 5, and whose determinant is nonzero mod 5. Let H be the subset of G consisting of all matrices whose determinant is 1 mod 5.
(a) How many elements are there in G and in H?
(b) Show that H is a normal subgroup of G.
(c) What familiar group is isomorphic to the quotient group G/H?

[**3**] Draw the Cayley graph of the group of order 10 defined using generators and relations by

$$G \quad = \quad \langle\, a, b \mid a^5 = 1,\ b^2 = 1,\ ba = ab \,\rangle.$$

What familiar group is isomorphic to G? Give an isomorphism.

[**4**] The *center* $Z(G)$ of a group G is the set of all elements of G which commute with every element of G:

$$Z(G) \quad = \quad \{\, g \in G \mid gh = hg \text{ for every } h \in G \,\}.$$

(a) Show that $Z(G)$ is a subgroup of G.
(b) Show that $Z(G)$ is in fact a normal subgroup of G.

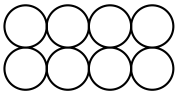


Figure 1

[**5**] How many ways are there of marking some (or none, or all) of the cells in Figure 1, up to symmetry? Consider two patterns to be the same if one can be obtained from the other by rotating or flipping. Use Burnside's formula

$$(\#\text{ of patterns up to symmetry}) \quad = \quad \frac{1}{|G|}\sum_{g\in G}(\#\text{ of patterns fixed by } g),$$

where G is the group of symmetries of this configuration of cells.

First midterm

Dave Bayer, Modern Algebra, October 14, 1998

Work as many parts of each problem as you can, while budgeting your time. For a successful exam, it isn't necessary to answer every part of every question.

[1] Let $G = S_3 = \{\, (),\ (1\ 2),\ (1\ 3),\ (2\ 3),\ (1\ 2\ 3),\ (1\ 3\ 2)\,\}$ be the symmetric group of all permutations of $\{\,1,\ 2,\ 3\,\}$, and let H be the subgroup $H = \{\, (\,),\ (1\ 2)\,\} \subset G$.
(a) List the left cosets of H in G.
(b) List the right cosets of H in G.
(c) Is H normal in G?

[2] Let m and n be relatively prime integers, and consider the two groups $G = \mathbb{Z}_m \times \mathbb{Z}_n$ and $H = \mathbb{Z}_{mn}$.
(a) Present each of these groups in terms of generators and relations.
(b) Find an isomorphism between G and H.
(c) Give an example showing what happens when m and n aren't relatively prime.

[3] Let G be the group presented in terms of generators and relations by

$$G \quad = \quad \langle\, a, b \mid a^2 = b^2 = 1,\ bab = aba \,\rangle.$$

Describe G as completely as you can. (Suggestions: How many elements does G have? List representatives for the distinct elements of G. Is G abelian or not? Draw the Cayley graph of G. Recognize G as isomorphic to a familiar group, and give an explicit isomorphism.)

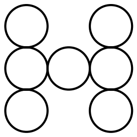


Figure 1

[4] Describe the group G of symmetries of the configuration of cells shown in Figure 1, considering both rotations and flips. How many ways are there of marking two of the cells in Figure 1, up to symmetry? Use Burnside's formula

$$(\text{\# of patterns up to symmetry}) \quad = \quad \frac{1}{|G|} \sum_{g \in G} (\text{\# of patterns fixed by } g).$$

[5] The *normalizer* $N(H)$ of a subgroup H of a group G can be defined to be the set

$$N(H) \quad = \quad \{\, g \in G \mid gHg^{-1} = H \,\}.$$

(a) Prove that $N(H)$ is a subgroup of G.
(b) Prove that H is a normal subgroup of $N(H)$.
(c) Suppose that J is another subgroup of G *conjugate* to H: $H \neq J$, but $aHa^{-1} = J$ for some $a \in G$. Describe the set $\{\, g \in G \mid gHg^{-1} = J \,\}$ in terms of a and $N(H)$.
(d) How many subgroups of G are conjugate to H, counting H itself?

Solutions to first midterm

Dave Bayer, Modern Algebra, Exam date October 14, 1998

[1] Let $G = S_3 = \{\, (),\ (1\ 2),\ (1\ 3),\ (2\ 3),\ (1\ 2\ 3),\ (1\ 3\ 2)\,\}$ be the symmetric group of all permutations of $\{\, 1,\ 2,\ 3\,\}$, and let H be the subgroup $H = \{\, (\,),\ (1\ 2)\,\} \subset G$.
(a) List the left cosets of H in G.

Solution: $H = \{\, (\,),\ (1\ 2)\,\}$ is one left coset. We expect a total of 3 left cosets, because the left cosets partition the 6 elements of G into 3 subsets of 2 elements each. The other left cosets are of the form gH for $g \in G$; we know that $g = (\,)$ and $g = (1\ 2)$ yield H itself, so we try another choice for g.

Taking $g = (1\ 3)$ we have $gH = \{\, (1\ 3),\ (1\ 3\ 2)\,\}$. (Calculation, working left to right to compute $(1\ 3)\ (1\ 2)$: 1 goes to 3 stays 3, 3 goes to 1 goes to 2, 2 stays 2 goes to 1, so $(1\ 3)\ (1\ 2) = (1\ 3\ 2)$.)

There are two elements of G unaccounted for, so the remaining left coset must be $\{\, (2\ 3),\ (1\ 2\ 3)\,\}$. Thus, the answer is

$$\{\, (\,),\ (1\ 2)\,\}, \quad \{\, (1\ 3),\ (1\ 3\ 2)\,\}, \quad \{\, (2\ 3),\ (1\ 2\ 3)\,\}.$$

(b) List the right cosets of H in G.

Solution: $H = \{\, (\,),\ (1\ 2)\,\}$ is one right coset; the other right cosets are of the form Hg. We have $H\ (1\ 3) = \{\, (1\ 3),\ (1\ 2\ 3)\,\}$, because $(1\ 2)\ (1\ 3) = (1\ 2\ 3)$, so the answer is

$$\{\, (\,),\ (1\ 2)\,\}, \quad \{\, (1\ 3),\ (1\ 2\ 3)\,\}, \quad \{\, (2\ 3),\ (1\ 3\ 2)\,\}.$$

(c) Is H normal in G?

Solution: No, because the left and right cosets of H in G aren't the same.

[2] Let m and n be relatively prime integers, and consider the two groups $G = \mathbb{Z}_m \times \mathbb{Z}_n$ and $H = \mathbb{Z}_{mn}$.
(a) Present each of these groups in terms of generators and relations.

$$G = \langle\, a, b \mid a^m = b^n = 1,\ ab = ba \,\rangle, \quad H = \langle\, c \mid c^{mn} = 1 \,\rangle$$

(b) Find an isomorphism between G and H.

Solution: The element ab of G has order mn, as does c, so we can define an isomorphism $f : H \to G$ by the rule $f(c) = ab$.

(c) Give an example showing what happens when m and n aren't relatively prime.

Solution: Taking $m = n = 2$, every nonidentity element of G (the Klein-four group) has order 2. Thus, G cannot be isomorphic to the cyclic group H, whose generator c has order 4.

[3] Let G be the group presented in terms of generators and relations by

$$G \quad = \quad \langle\, a, b \mid a^2 = b^2 = 1,\ bab = aba \,\rangle.$$

Describe G as completely as you can. (Suggestions: How many elements does G have? List representatives for the distinct elements of G. Is G abelian or not? Draw the Cayley graph of G. Recognize G as isomorphic to a familiar group, and give an explicit isomorphism.)

Solution: Using the rules $a^2 = 1$ and $b^2 = 1$, we can simplify any word in G so it has no repeated letters. In other words, we can simplify to words which alternate $ababab\ldots$ or $bababa\ldots$. For example, $baabab = b(aa)bab = b(1)bab = bbab = (bb)ab = (1)ab = ab$. Moreover, we can change any bab to aba as a way of standardizing words.

Playing around, we can find a bab in any alternating word of length ≥ 4, and after replacing bab by aba there will always be a repeated letter we can simplify. For example, $abab$ becomes $a(bab) = a(aba) = (aa)ba = ba$, and $baba$ becomes $(bab)a = (aba)a = ab(aa) = ab$. We can also always change bab to aba. With these simplifications, G consists of the identity 1, the words a, ab, aba which start with a, and the words b and ba which start with b. Thus G has 6 elements, and representatives for these 6 elements can be chosen as follows:

$$G \quad = \quad \{\,1,\ a,\ ab,\ aba,\ b,\ ba\,\}.$$

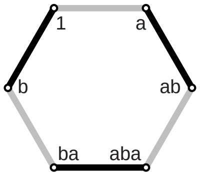


Figure 1

In figure 1 we draw a Cayley graph of G, where moving either way along a grey edge corresponds to right multiplication by a, and moving either way along a black edge corresponds to right multiplication by b. Starting at 1, there are two ways to reach $bab = aba$: the path bab (b then a then b) which goes counterclockwise from 1 to aba, and the path aba (a then b then a) which goes clockwise from 1 to aba.

G is not abelian, because $ab \neq ba$. There is only one nonabelian group of order 6, up to isomorphism: the group S_3 of all permutations of 1, 2, 3, which we have also encountered as the group of symmetries of a triangle. For an explicit isomorphism, identity a with (1 2), and identify b with (1 3). Then $a^2 = b^2 = 1$ as desired. Now check that $bab = aba$: $bab = (1\ 3)(1\ 2)(1\ 3) = (2\ 3)$, and $aba = (1\ 2)(1\ 3)(1\ 2) = (2\ 3)$.

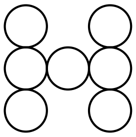


Figure 2

[4] Describe the group G of symmetries of the configuration of cells shown in Figure 2, considering both rotations and flips. How many ways are there of marking two of the cells in Figure 1, up to symmetry? Use Burnside's formula

$$(\#\text{ of patterns up to symmetry}) \quad = \quad \frac{1}{|G|}\sum_{g\in G}(\#\text{ of patterns fixed by } g).$$

Solution: This configuration is preserved by leaving it alone, flipping it horizontally or vertically, or rotating it a half turn. Thus G has 4 elements.

There are $\frac{7\cdot 6}{2\cdot 1} = 21$ ways of choosing 2 of the 7 cells, all of which are fixed by the identity.

To count patterns which are preserved by flipping across a horizontal axis, we can choose the outer left corners, the outer right corners, or any two of the three cells in the middle row. This gives $1+1+3 = 5$ possibilities.

To count patterns which are preserved by flipping across a vertical axis, we can choose one cell in the left column, and its counterpart in the right column under flipping. This gives 3 possibilities.

To count patterns which are preserved by rotating a half turn, we can choose one cell in the left column, and its counterpart in the right column under rotating. This gives 3 possibilities.

Thus, by Burnside's formula there are $(21 + 5 + 3 + 3)/4 = 8$ patterns, up to symmetry.

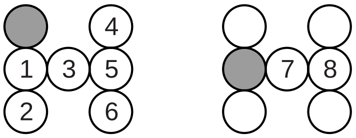


Figure 3

To check our work, we use figure 3 to confirm that there are 8 patterns up to symmetry. If any corner is marked, we can move the pattern so the upper left corner is marked, as shown on the left. Then, any of the remaining 6 cells can be marked as our second choice, and each of these patterns are different. We must also count patterns which don't mark any corner: There is only one center cell, so such patterns must mark a side cell. We can move the pattern so the left side cell is always marked, as shown on the right. There are 2 noncorner cells left for our second choice, and they give different patterns, for a total of 8.

[5] The *normalizer* $N(H)$ of a subgroup H of a group G can be defined to be the set

$$N(H) \quad = \quad \{\, g \in G \mid gHg^{-1} = H \,\}.$$

(a) Prove that $N(H)$ is a subgroup of G.

Solution: We need to check that $N(H)$ is closed under multiplication, and under taking inverses. If a, $b \in N(H)$, then $aHa^{-1} = H$ and $bHb^{-1} = H$. Then $(ab)H(ab)^{-1} = abHb^{-1}a^{-1} = aHa^{-1} = H$, so $ab \in N(H)$, and $N(H)$ is closed under multiplication. Also, multiplying $aHa^{-1} = H$ on the left by a^{-1} and on the right by a yields $H = a^{-1}Ha$, showing that $a^{-1} \in N(H)$, so $N(H)$ is closed under taking inverses.

(b) Prove that H is a normal subgroup of $N(H)$.

Solution: We already know that H is a group, because it is a subgroup of G. H is contained in $N(H)$ because $gHg^{-1} = H$ for every $g \in H$. Thus, H is a subgroup of $N(H)$. H is normal in $N(H)$ because $gHg^{-1} = H$ for every $g \in N(H)$, by the definition of $N(H)$.

(c) Suppose that J is another subgroup of G *conjugate* to H: $H \neq J$, but $aHa^{-1} = J$ for some $a \in G$. Describe the set $\{\, g \in G \mid gHg^{-1} = J \,\}$ in terms of a and $N(H)$.

Solution: Let $U = \{\, g \in G \mid gHg^{-1} = J \,\}$. Then U is the left coset $aN(H)$ of $N(H)$: If $g \in aN(H)$, then $g = ab$ for some $b \in N(H)$, so $gHg^{-1} = abHb^{-1}a^{-1} = aHa^{-1} = J$, so $g \in U$. Conversely, if $g \in U$, then $a^{-1}gHg^{-1}a = a^{-1}Ja = H$, so $a^{-1}g \in N(H)$, so $g = aa^{-1}g \in aN(H)$.

(d) How many subgroups of G are conjugate to H, counting H itself?

Solution: The subgroups J of G conjugate to H correspond 1:1 to the cosets $aN(H)$ of $N(H)$ in G, by part (c) above. The coset $N(H)$ itself counts the subgroup H itself. Thus, the number of conjugate subgroups is equal to the number of cosets, which is the index of $N(H)$ in G.

Practice problems for second midterm

Dave Bayer, Modern Algebra, November 5, 1997

There will be two review sessions in 528 Mathematics: Friday, November 7 at 2:40pm, and Sunday, November 9 at 2:40pm. (We will move if we need more space.)

[**1**] Define an abstract field, and a vector space over an abstract field. Define a homomorphism of abstract fields, and a homomorphism of vector spaces.

[**2**] Let p be a prime, and let $\mathbf{F}_p = \mathbb{Z}/p\mathbb{Z}$ be the finite field with p elements.

(a) What is the order of the group of invertible elements of $\mathbf{F}_p$?

(b) Find the multiplicative inverse of 17 mod 31, by either using the extended Euclidean algorithm, or by taking successive powers.

[**3**] Let p and q be primes, and let $\mathbb{Z}/pq\mathbb{Z}$ be the ring of integers modulo pq.

(a) What is the order of the group of invertible elements of $\mathbb{Z}/pq\mathbb{Z}$?

(b) Find the multiplicative inverse of 17 mod 91, by either using the extended Euclidean algorithm, or by taking successive powers.

[**4**] Let the linear transformation $T : \mathbb{R}^2 \to \mathbb{R}^2$ be given by the matrix $A = \begin{bmatrix} 1 & 1 \\ -1 & -1 \end{bmatrix}$ with respect to the standard basis for $\mathbb{R}^2$.

(a) Find a matrix $B = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$, $\begin{bmatrix} a & 1 \\ 0 & a \end{bmatrix}$, or $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ which is similar to A.

(b) Find a basis v_1, v_2 for $\mathbb{R}^2$ such that the matrix for T with respect to this basis is B.

The following problems each involve working with linearly independent sets, spanning sets, or bases.

[**5**] Let V be a finite-dimensional vector space over a field F, and suppose that $v_1, \ldots, v_n$ spans V. Prove that $v_1, \ldots, v_n$ contains a basis of V.

[**6**] Let V be a finite-dimensional vector space over a field F, and suppose that $v_1, \ldots, v_n$ are linearly independent vectors in V. Prove that $v_1, \ldots, v_n$ can be extended to a basis of V.

[**7**] Let V be a finite-dimensional vector space over a field F, and suppose that $v_1, \ldots, v_m$ and $w_1, \ldots, w_n$ are two bases of V. Prove that $m = n$.

[**8**] Let V and W be finite-dimensional vector spaces over a field F, and let $A : V \to W$ be a linear transformation. Prove that

$$\dim(V) \quad = \quad \dim(\ker A) \; + \; \dim(\operatorname{im} A).$$

[9] Let W_1 and W_2 be two subspaces of a finite-dimensional vector space V over a field F. Prove that

$$\dim(W_1) \;+\; \dim(W_2) \quad = \quad \dim(W_1 \cap W_2) \;+\; \dim(W_1 + W_2).$$

[10] Let W_1, W_2 and W_3 be three subspaces of a finite-dimensional vector space V over a field F. Prove that

$$\dim(W_1 + W_2 + W_3) \quad \leq \quad \dim(W_1) \;+\; \dim(W_2) \;+\; \dim(W_3).$$

[11] Let V be a finite-dimensional vector space over a field F, and let $A : V \to V$ be a linear transformation such that $A^2 = 0$. In other words, we have

$$V \xrightarrow{\;\;A\;\;} \operatorname{im} A \xrightarrow{\;\;A\;\;} 0.$$

(a) Find a basis $v_1, \ldots, v_n$ for V, such that the matrix for A with respect to this basis is block diagonal with blocks $[0]$ or $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$. Prove that $v_1, \ldots, v_n$ is in fact a basis for V.

(b) Show that $\dim(\operatorname{im} A) \leq \frac{1}{2}\dim(V)$.

[12] Let V be a finite-dimensional vector space over a field F, and let $A : V \to V$ be a linear transformation such that $A^3 = 0$.

(a) Find a basis $v_1, \ldots, v_n$ for V, such that the matrix for A with respect to this basis is block diagonal with blocks $[0]$, $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$, or $\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}$. Prove that $v_1, \ldots, v_n$ is in fact a basis for V.

(b) What bounds must hold between the dimensions $\dim(V)$, $\dim(\operatorname{im} A)$, and $\dim(\operatorname{im} A^2)$?

[13] Let V be a finite-dimensional vector space over a field F, and let $A : V \to V$ be a linear transformation such that $\dim(\operatorname{im} A) < \dim(V)$, but $\operatorname{im} A^2 = \operatorname{im} A$. In other words, the restriction of the linear transformation $A : \operatorname{im} A \to \operatorname{im} A$ is nonsingular (an isomorphism).

Let $n = \dim(V)$, and $m = \dim(\operatorname{im} A)$. Find a basis $v_1, \ldots, v_m, \ldots, v_n$ for V, such that the matrix for A with respect to this basis has all zero entries outside of an m by m diagonal block corresponding to the subspace $\operatorname{im} A$.

Second midterm

Dave Bayer, Modern Algebra, November 9, 1997

Please solve 5 of the following 6 problems. Each problem is worth 5 points for a total of 25 points. I will also award up to 5 bonus points (recorded separately) for particularly impressive examinations.

[1] Define a *vector space*. Define a *spanning set*, a *linearly independent set*, and a *basis*. Define the *dimension* of a vector space.

[2] Let $\mathbf{F}_{31991} = \mathbb{Z}/31991\mathbb{Z}$ be the finite field with 31991 elements.

(a) What is the order of the group of invertible elements of $\mathbf{F}_{31991}$?

(b) Find the multiplicative inverse of 2 mod 31991, any way you can. Check your answer.

[3] Let V be a finite-dimensional vector space over a field F, and suppose that $v_1, \ldots, v_n$ spans V. Prove that $v_1, \ldots, v_n$ contains a basis of V.

[4] Let V and W be finite-dimensional vector spaces over a field F, and let $A : V \to W$ be a linear transformation. Prove that

$$\dim(V) \quad = \quad \dim(\ker A) \;+\; \dim(\operatorname{im} A).$$

[5] Let $W_1, \ldots, W_n$ be n subspaces of a finite-dimensional vector space V over a field F. Prove that

$$\dim(W_1 + \ldots + W_n) \quad \leq \quad \dim(W_1) \;+\; \ldots \;+\; \dim(W_n).$$

[6] Let V be an n-dimensional vector space over a field F, and let $A : V \to V$ be a linear transformation such that $A^2 = 0$. Find a basis

$$v_1, \ldots, v_m, \quad v_{m+1}, \ldots, v_{2m}, \quad v_{2m+1}, \ldots, v_n$$

for V, such that

$Av_i = 0$ for $i = 1, \ldots m$,
$Av_i = v_{i-m}$ for $i = m+1, \ldots, 2m$,
$Av_i = 0$ for $i = 2m+1, \ldots n$.

Prove that $v_1, \ldots, v_n$ is a basis for V.

Second midterm

Dave Bayer, Modern Algebra, November 18, 1998

[1] Find the multiplicative inverse of 23 mod 103.

[2] *Prove* **ONE** *of the following two assertions:*

(a) Let V and W be subspaces of a vector space U. Then

$$\dim(V) \ + \ \dim(W) \quad = \quad \dim(V \cap W) \ + \ \dim(V + W).$$

(b) Let $T : V \rightarrow W$ be a linear transformation of vector spaces. Then

$$\dim(\ker(T)) \ + \ \dim(\mathrm{image}(T)) \quad = \quad \dim(V).$$

[3] Let

$$A = \begin{bmatrix} 5 & -4 \\ 1 & 1 \end{bmatrix}.$$

Find a change of basis matrix B so $A = B\,C\,B^{-1}$ where C is in Jordan canonical form. Use B and C to give an expression for e^{At}. You do not need to multiply this expression out.

[4] Let $T : V \rightarrow V$ be a linear transformation from the n-dimensional vector space V to itself, such that $T^2 = 0$. Prove that for some basis $\mathbf{v}_1, \ldots, \mathbf{v}_n$ of V, the matrix A for T with respect to this basis is in Jordan canonical form.

[5] Let

$$A = \begin{bmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{bmatrix}.$$

Find a formula for e^{At}.

Solutions to second midterm

Dave Bayer, Modern Algebra, Exam date November, 1998

[1] Find the multiplicative inverse of 23 mod 103.

Solution: By the extended euclidean algorithm, we compute

$$\begin{bmatrix} 103 & 1 & 0 \\ 23 & 0 & 1 \\ 11 & 1 & -4 \\ 1 & -2 & 9 \end{bmatrix} \quad \text{which we interpret as} \quad \begin{bmatrix} 103 = 1 \cdot 103 + 0 \cdot 23 \\ 23 = 0 \cdot 103 + 1 \cdot 23 \\ 11 = 1 \cdot 103 - 4 \cdot 23 \\ 1 = -2 \cdot 103 + 9 \cdot 23 \end{bmatrix}$$

so $23^{-1} = 9$ mod 103. We check our answer: $23 \cdot 9 = 230 - 23 = 207 = (2 \cdot 103) + 1$.

Alternatively, the multiplicative group of integers mod 103 has order 102 because 103 is prime, so $x \cdot x^{101} = x^{102} = 1$ for any integer x which is nonzero mod 103. Writing $101 = 64 + 32 + 4 + 1$, we can compute x^{101} as $x^{64} \cdot x^{32} \cdot x^4 \cdot x$. We compute $23^{-1} = 23^{101}$ by hand, reducing mod 103 whenever it helps:

$$\begin{aligned}
23^2 &= (25-2)^2 = 625 - 4 \cdot 25 + 4 = 529 = 14 \\
23^4 &= 14^2 = (15-1)^2 = 225 - 2 \cdot 15 + 1 = 196 = -10 \\
23^8 &= (-10)^2 = 100 = -3 \\
23^{16} &= (-3)^2 = 9 \\
23^{32} &= 9^2 = 81 = -22 \\
23^{64} &= (-22)^2 = 4 \cdot 11^2 = 4 \cdot 121 = 4 \cdot 18 = 72 = -31 \\
23^{-1} &= 23^{101} = 23^{64} \cdot 23^{32} \cdot 23^4 \cdot 23 = (-31)(-22)(-10)23 = -(620+62)230 \\
&= -(2+62)24 = -64 \cdot 24 = -16 \cdot 96 = 16 \cdot 7 = 80 + 32 = 112 = 9
\end{aligned}$$

We have used several times the formula $(a-b)^2 = a^2 - 2ab + b^2$ to rewrite squares into products we can recall without the tedium of direct multiplication. We chose negative representatives mod 103 whenever they had a smaller magnitude. The point is to meander through the arithmetic, keeping sufficiently amused to avoid making mistakes. It is unlikely that any two people would follow the same course through this calculation.

Can you think of a way of computing x^{101} that takes fewer than the 9 multiplies

$$x^2 = x \cdot x, \quad x^4 = x^2 \cdot x^2, \quad x^8 = x^4 \cdot x^4, \quad x^{16} = x^8 \cdot x^8, \quad x^{32} = x^{16} \cdot x^{16}, \quad x^{64} = x^{32} \cdot x^{32},$$

$$x^5 = x \cdot x^4, \quad x^{37} = x^5 \cdot x^{32}, \quad x^{101} = x^{37} \cdot x^{64}$$

used here? What about for other powers of x? How would you teach a computer to exponentiate, if multiplication was *extremely* expensive, and you were allowed all the preparation time you needed to plan the calculation?

[2] *Prove* **ONE** *of the following two assertions:*

(a) Let V and W be subspaces of a vector space U. Then

$$\dim(V) + \dim(W) = \dim(V \cap W) + \dim(V + W).$$

Solution: Choose a basis $u_1, \ldots, u_j$ for $V \cap W$. Extend $u_1, \ldots, u_j$ to a basis $u_1, \ldots, u_j, v_1, \ldots, v_k$ for V. Also extend $u_1, \ldots, u_j$ to a basis $u_1, \ldots, u_j, w_1, \ldots, w_\ell$ for W. We claim that $u_1, \ldots, u_j, v_1, \ldots, v_k, w_1, \ldots, w_\ell$ is a basis for $V + W$. Counting basis elements, the formula will follow as

$$(j+k) \; + \; (j+\ell) \quad = \quad (j) \; + \; (j+k+\ell).$$

Independence: For any expression

$$\sum_{i=1}^{j} r_i\, u_i \; + \; \sum_{i=1}^{k} s_i\, v_i \; + \; \sum_{i=1}^{\ell} t_i\, w_i \quad = \quad 0$$

we need to show that all coefficients r_i, s_i, t_i are zero. Write

$$\alpha \quad = \quad \sum_{i=1}^{j} r_i\, u_i \; + \; \sum_{i=1}^{k} s_i\, v_i \quad = \quad -\sum_{i=1}^{\ell} t_i\, w_i.$$

We see that $\alpha \in V$ and $\alpha \in W$, so $\alpha \in V \cap W$. Since $u_1, \ldots, u_j$ is a basis for $V \cap W$, α can be written in a unique way as a linear combination of $u_1, \ldots, u_j$. This same expression must be the unique way of writing α as a linear combination of the basis $u_1, \ldots, u_j, w_1, \ldots, w_\ell$ for W, so we have $t_1 = \ldots = t_\ell = 0$. Thus $\alpha = 0$. Because $u_1, \ldots, u_j, v_1, \ldots, v_k$ is a basis for V, we have $r_1 = \ldots = r_j = 0$ and $s_1 = \ldots = s_k = 0$ as desired.

Spanning: If $u \in V + W$, we need to show that u can be written as a linear combination of the vectors $u_1, \ldots, u_j, v_1, \ldots, v_k, w_1, \ldots, w_\ell$. Write $u = v + w$ where $v \in V$ and $w \in W$, and write

$$v \quad = \quad \sum_{i=1}^{j} r_i\, u_i \; + \; \sum_{i=1}^{k} s_i\, v_i \quad \text{and} \quad w \quad = \quad \sum_{i=1}^{j} r'_i\, u_i \; + \; \sum_{i=1}^{\ell} t_i\, w_i.$$

Then

$$u \quad = \quad v + w \quad = \quad \sum_{i=1}^{j} (r_i + r'_i)\, u_i \; + \; \sum_{i=1}^{k} s_i\, v_i \; + \; \sum_{i=1}^{\ell} t_i\, w_i$$

as desired.

(b) Let $T : V \to W$ be a linear transformation of vector spaces. Then

$$\dim(\ker(T)) \; + \; \dim(\mathrm{image}(T)) \quad = \quad \dim(V).$$

Solution: There are various ways to prove this; here is one: Choose a basis $u_1, \ldots, u_j$ for $\ker(T)$, and choose a basis $w_1, \ldots, w_k$ for $\mathrm{image}(T)$. For each $w_i \in W$, choose a vector $v_i \in V$ so $T(v_i) = w_i$. We claim that $u_1, \ldots, u_j, v_1, \ldots, v_k$ is a basis for V. Counting basis elements, the formula will follow as

$$(j) \; + \; (k) \quad = \quad (j+k).$$

Independence: For any expression

$$\sum_{i=1}^{j} r_i\, u_i \; + \; \sum_{i=1}^{k} s_i\, v_i \quad = \quad 0$$

we need to show that all coefficients r_i, s_i are zero. Applying T, we have

$$T\left(\sum_{i=1}^{j} r_i\, u_i \;+\; \sum_{i=1}^{k} s_i\, v_i\right) \quad=\quad 0 \;+\; \sum_{i=1}^{k} s_i\, T(v_i) \quad=\quad \sum_{i=1}^{k} s_i\, w_i \quad=\quad 0,$$

so $s_i = \ldots = s_k = 0$ because $w_1, \ldots, w_k$ is a basis for image(T). Now $r_i = \ldots = r_j = 0$ because $u_1, \ldots, u_j$ is a basis for $\ker(T)$.

Spanning: If $v \in V$, we need to show that v can be written as a linear combination of the vectors $u_1, \ldots, u_j, v_1, \ldots, v_k$. Write $T(v) = \sum_{i=1}^{k} s_i\, w_i$. Then $T(v) = T(\sum_{i=1}^{k} s_i\, v_i)$, so $v - \sum_{i=1}^{k} s_i\, v_i$ belongs to $\ker(T)$. Write

$$v - \sum_{i=1}^{k} s_i\, v_i = \sum_{i=1}^{j} r_i\, u_i, \qquad \text{so} \quad v = \sum_{i=1}^{j} r_i\, u_i \;+\; \sum_{i=1}^{k} s_i\, v_i \quad \text{as desired.}$$

[3] Let

$$A = \begin{bmatrix} 5 & -4 \\ 1 & 1 \end{bmatrix}.$$

Find a change of basis matrix B so $A = B\,C\,B^{-1}$ where C is in Jordan canonical form. Use B and C to give an expression for e^{At}. You do not need to multiply this expression out.

Solution: A has characteristic polynomial

$$\lambda^2 - \text{trace(A)}\lambda + \det(A) \quad=\quad \lambda^2 - 6\lambda + 9 = (\lambda - 3)^2,$$

so A has a repeated eigenvalue of 3. We have

$$A - 3I \quad=\quad \begin{bmatrix} 2 & -4 \\ 1 & -2 \end{bmatrix}$$

which is a nonzero matrix, so we have the Jordan canonical forms

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \quad \text{for} \quad A - 3I, \qquad \text{and} \qquad \begin{bmatrix} 3 & 1 \\ 0 & 3 \end{bmatrix} \quad \text{for} \quad A,$$

with respect to any basis v_1, v_2 such that

$$(A - 3I)\, v_2 \quad=\quad v_1 \qquad \text{and} \qquad (A - 3I)\, v_1 \quad=\quad 0.$$

This will hold for most choices of v_2, so we try $v_2 = (1, 0)$. We have $(A - 3I)(1, 0) = (2, 1)$, and $(A - 3I)(2, 1) = (0, 0)$ as desired. Thus

$$A \;=\; \begin{bmatrix} 5 & -4 \\ 1 & 1 \end{bmatrix} \;=\; \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 3 & 1 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix}.$$

We check our work:

$$\begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix} \;=\; \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \text{and} \quad \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 3 & 1 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix} \;=\; \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 3 & -6 \end{bmatrix} \;=\; \begin{bmatrix} 5 & -4 \\ 1 & 1 \end{bmatrix}.$$

It follows that

$$e^{At} \;=\; \begin{bmatrix} 5 & -4 \\ 1 & 1 \end{bmatrix} \;=\; \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} e^{3t} & te^{3t} \\ 0 & e^{3t} \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix}.$$

[4] Let $T : V \to V$ be a linear transformation from the n-dimensional vector space V to itself, such that $T^2 = 0$. Prove that for some basis $\mathbf{v}_1, \ldots, \mathbf{v}_n$ of V, the matrix A for T with respect to this basis is in Jordan canonical form.

Solution: We have image$(T) \subset \ker(T)$, because $w \in$ image$(T) \Rightarrow w = T(v) \Rightarrow T(w) = T^2(v) = 0$. Choose a basis $w_1, \ldots, w_j$ for image(T), and extend this basis to a basis $w_1, \ldots, w_j, u_1, \ldots, u_k$ for $\ker(T)$. For each w_i, choose a vector $v_i \in V$ so $T(v_i) = w_i$. We claim that $w_1, \ldots, w_j, u_1, \ldots, u_k, v_1, \ldots, v_j$ is a basis for V. Arranging this basis in the order $v_1, w_1, \ldots, v_j, w_j, u_1, \ldots, u_k$ and relabeling as $\mathbf{v}_1, \ldots, \mathbf{v}_n$ gives the desired Jordan form.
Independence: For any expression

$$\sum_{i=1}^{j} r_i\, w_i \;+\; \sum_{i=1}^{k} s_i\, u_i \;+\; \sum_{i=1}^{j} t_i\, v_i \;\;=\;\; 0$$

we need to show that all coefficients r_i, s_i, t_i are zero. Applying T, we have

$$T\left(\sum_{i=1}^{j} r_i\, w_i \;+\; \sum_{i=1}^{k} s_i\, u_i \;+\; \sum_{i=1}^{j} t_i\, v_i\right) \;\;=\;\; 0 \;+\; 0 \;+\; \sum_{i=1}^{j} t_i\, T(v_i) \;\;=\;\; \sum_{i=1}^{j} y_i\, w_i \;\;=\;\; 0,$$

so $t_i = \ldots = t_j = 0$ because $w_1, \ldots, w_k$ is a basis for image(T). Now $r_i = \ldots = r_j = 0$ and $s_i = \ldots = s_k = 0$ because $w_1, \ldots, w_j, u_1, \ldots, u_k$ is a basis for $\ker(T)$.
Spanning: If $v \in V$, we need to show that v can be written as a linear combination of the vectors $u_1, \ldots, u_j, v_1, \ldots, v_k$. Write $T(v) = \sum_{i=1}^{j} t_i\, w_i$. Then $T(v) = T(\sum_{i=1}^{j} t_i\, v_i)$, so $v - \sum_{i=1}^{j} t_i\, v_i$ belongs to $\ker(T)$. Write

$$v - \sum_{i=1}^{j} t_i\, v_i = \sum_{i=1}^{j} r_i\, w_i \;+\; \sum_{i=1}^{k} s_i\, u_i,$$

so

$$v \;\;=\;\; \sum_{i=1}^{j} r_i\, w_i \;+\; \sum_{i=1}^{k} s_i\, u_i \;+\; \sum_{i=1}^{j} t_i\, v_i$$

as desired.

[5] Let

$$A = \begin{bmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{bmatrix}.$$

Find a formula for e^{At}.

Solution: We first need a formula for A^n. We have

$$A^1 = \begin{bmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{bmatrix},\; A^2 = \begin{bmatrix} \lambda^2 & 2\lambda & 1 \\ 0 & \lambda^2 & 2\lambda \\ 0 & 0 & \lambda \end{bmatrix},\; A^3 = \begin{bmatrix} \lambda^3 & 3\lambda^2 & 3\lambda \\ 0 & \lambda^3 & 3\lambda^2 \\ 0 & 0 & \lambda \end{bmatrix},\; A^4 = \begin{bmatrix} \lambda^4 & 4\lambda^3 & 6\lambda^2 \\ 0 & \lambda^4 & 4\lambda^3 \\ 0 & 0 & \lambda \end{bmatrix},\; A^5 = \begin{bmatrix} \lambda^5 & 5\lambda^4 & 10\lambda^3 \\ 0 & \lambda^5 & 5\lambda^4 \\ 0 & 0 & \lambda \end{bmatrix}$$

allowing us to guess that

$$A^n = \begin{bmatrix} \lambda^n & n\lambda^{n-1} & \frac{n(n-1)}{2}\lambda^{n-2} \\ 0 & \lambda^n & n\lambda^{n-1} \\ 0 & 0 & \lambda^n \end{bmatrix}$$

We check this formula inductively:

$$A^{n+1} = A\,A^n = \begin{bmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{bmatrix} \begin{bmatrix} \lambda^n & n\lambda^{n-1} & \frac{n(n-1)}{2}\lambda^{n-2} \\ 0 & \lambda^n & n\lambda^{n-1} \\ 0 & 0 & \lambda^n \end{bmatrix} = \begin{bmatrix} \lambda^{(n+1)} & (n+1)\lambda^n & \frac{(n+1)n}{2}\lambda^{n-1} \\ 0 & \lambda^{(n+1)} & (n+1)\lambda^n \\ 0 & 0 & \lambda^{(n+1)} \end{bmatrix}$$

as desired. Now,

$$\begin{aligned} e^{At} &= \sum_{n=0}^{\infty} A^n \frac{t^n}{n!} = \sum_{n=0}^{\infty} \begin{bmatrix} \lambda^n & n\lambda^{n-1} & \frac{n(n-1)}{2}\lambda^{n-2} \\ 0 & \lambda^n & n\lambda^{n-1} \\ 0 & 0 & \lambda^n \end{bmatrix} \frac{t^n}{n!} \\ &= \begin{bmatrix} \sum_{n=0}^{\infty} \frac{\lambda^n t^n}{n!} & \sum_{n=0}^{\infty} \frac{n\lambda^{n-1} t^n}{n!} & \sum_{n=0}^{\infty} \frac{\frac{n(n-1)}{2}\lambda^{n-2} t^n}{n!} \\ 0 & \sum_{n=0}^{\infty} \frac{\lambda^n t^n}{n!} & \sum_{n=0}^{\infty} \frac{n\lambda^{n-1} t^n}{n!} \\ 0 & 0 & \sum_{n=0}^{\infty} \frac{\lambda^n t^n}{n!} \end{bmatrix} \end{aligned}$$

Now,

$$\begin{aligned} \sum_{n=0}^{\infty} \frac{\lambda^n t^n}{n!} &= e^{\lambda t} \\ \sum_{n=0}^{\infty} \frac{n\lambda^{n-1} t^n}{n!} &= t\sum_{n=1}^{\infty} \frac{\lambda^{n-1} t^{n-1}}{(n-1)!} = t\sum_{n=0}^{\infty} \frac{\lambda^n t^n}{n!} = t\,e^{\lambda t} \\ \sum_{n=0}^{\infty} \frac{\frac{n(n-1)}{2}\lambda^{n-2} t^n}{n!} &= \frac{t^2}{2}\sum_{n=2}^{\infty} \frac{\lambda^{n-2} t^{n-2}}{(n-2)!} = \frac{t^2}{2}\sum_{n=0}^{\infty} \frac{\lambda^n t^n}{n!} = \frac{t^2}{2}\,e^{\lambda t} \end{aligned}$$

so

$$e^{At} = \begin{bmatrix} e^{\lambda t} & te^{\lambda t} & \frac{t^2}{2}e^{\lambda t} \\ 0 & e^{\lambda t} & te^{\lambda t} \\ 0 & 0 & e^{\lambda t} \end{bmatrix}$$

giving us the desired formula.

Practice problems for final

Dave Bayer, Modern Algebra, November 5, 1997

These practice problems cover material in Chapters 5 and 6. Also review the practice problems given for the two midterms, and the two midterms.

[**1**] Let G be a group of order $|G| = ab$, and let $\mathcal{S}$ be the set of all subsets of G of order a.
(a) Give a formula for $N = |\mathcal{S}|$ as a binomial coefficient.
(b) Show that $\gcd(a, N) = \gcd(a, b)$.
(c) If a and b are relatively prime, show that a and N are relatively prime.
(d) If $a = p^e$ for a prime p, and p doesn't divide b, show that p doesn't divide N.

[**2**] Let $G = \mathbb{Z}_4 = \{0, 1, 2, 3\}$ be the group of integers mod 4, under addition. Let $\mathcal{S}$ be the set of all subsets of G of order 2.
(a) What is $N = |\mathcal{S}|$ in this case?
(b) List the elements of $\mathcal{S}$.
(c) Let G act on the subsets of $\mathcal{S}$ by addition. What are the orbits of this action?

[**3**] Let $G = \{1, a, b, c\}$ be the Klein-4 group, where

$$a^2 = b^2 = c^2 = 1, \quad ab = ba = c, \quad ac = ca = b, \quad bc = cb = a.$$

Let $\mathcal{S}$ be the set of all subsets of G of order 2.
(a) What is $N = |\mathcal{S}|$ in this case?
(b) List the elements of $\mathcal{S}$.
(c) Let G act on the subsets of $\mathcal{S}$ by left multiplication. What are the orbits of this action?

Final Examination

Dave Bayer, Modern Algebra, December 23, 1998

Each problem is worth 5 points for a total of 50 points. Work as much of each problem as you can.

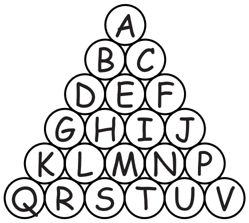


Figure 1

[**1**] Let the dihedral group D_3 of symmetries of the triangle act on the cells shown in Figure 1. For example, a vertical axis flip takes cell B to cell C, and a clockwise rotation takes cell B to cell P.

What are the orbits of D_3, acting on the set of cells

$$\{A, B, C, D, E, F, G, H, I, J, K, L, M, N, P, Q, R, S, T, U, V\}?$$

[**2**] Let a, b be two elements of a group G, and let H be a subgroup of G. Consider the left cosets aH and bH of H in G. Show that if aH and bH have any elements in common, then $aH = bH$.

[**3**] The *center* Z of a group G is the set of elements of G which commute with all elements of G:

$$Z = \{\ g \in G \ \mid \ gh = hg \text{ for all } h \in G\ \}.$$

The *centralizer* $Z(x)$ of an element $x \in G$ is the set of elements of G which commute with x:

$$Z(x) = \{\ g \in G \ \mid \ gx = xg\ \}.$$

(a) Show that $Z(x)$ is a subgroup of G.

(b) Show that $x \in Z$ if and only if $Z(x) = G$.

[**4**] The centralizer $Z(x)$ of $x \in G$ can also be thought of as the stabilizer of x with respect to conjugation:

$$Z(x) = \{\ g \in G \ \mid \ gxg^{-1} = x\ \}.$$

Suppose that $axa^{-1} = y$ for some $a \in G$, so x and y are conjugate elements of G.

(a) Describe the subset $\{\ g \in G \ \mid \ gxg^{-1} = y\ \}$ in terms of $Z(x)$ and a.

(b) Show that the number of elements of G conjugate to x is given by the formula $|G| \,/\, |Z(x)|$.

(c) Show that any group of order p^2 is abelian, when p is prime.

[**5**] Let U, V, and W be three subspaces of a finite-dimensional vector space over a field F. Prove that

$$\dim(U + V + W) \ \leq\ \dim(U) \ +\ \dim(V) \ +\ \dim(W).$$

[**6**] Find the multiplicative inverse of 102 mod 103.

[**7**] Let

$$A = \begin{bmatrix} 2 & 0 \\ 1 & 2 \end{bmatrix}.$$

Find a change of basis matrix B so $A = B\,C\,B^{-1}$ where C is in Jordan canonical form. Use B and C to find e^{At}.

[**8**] Let $G = \{1, a, a^2, b, ab, a^2b\} = \langle\, a, b \mid a^3 = b^2 = 1,\ ba = a^{-1}b \,\rangle$; this is a presentation of the dihedral group D_3. Let $U = \{a, a^2, ab, a^2b\} \subset G$, and let G act on itself by left multiplication.

(a) What is the stabilizer $H = \text{Stab}(U)$ of U?

(b) List the right cosets Ha of H in G.

(c) Express U as a union of right cosets of H, and verify that $|H|$ divides $|U|$.

[**9**] Let G be a group of order $p^e\,m$, where p is a prime that does not divide m. Prove that G has a subgroup H of order p^e.

[**10**] Classify the groups of order n, where

(a) n = 33.

(b) n = 39.

(c) n = 49.