MATHEMATICS 152, FALL 2004
METHODS OF DISCRETE MATHEMATICS
Homework Problems relevant to the second quiz

Last modified: October 15, 2004

Reading

- Biggs, Chapter 22.
- Biggs, Chapter 23, especially 23.1–23.4.
- The handout on Affine Geometry.

Required Problems

Due dates are subject to minor adjustments, since they are based on guesses about how far we will get in class.

The second quiz will be on Thursday, November 18, not on November 9 as shown on the schedule in the syllabus.

Problems due Tuesday, Oct. 26

1. Show that $H = \{I, (12)\}$ is not a normal subgroup of S_4 by computing its conjugate subgroups.
2. Show that $J = \{I, (123), (132)\}$ is a normal subgroup of S_3 by computing its conjugate subgroups. What is the quotient group S_3/J?
3. Consider the group $G = (\mathbb{Z}_{13}^{\times}, \otimes)$ and the subgroup H generated by [4]. Determine the quotient group G/H by writing down its elements (the cosets) and writing a group table for them.
4. Consider the ring $R = M_2(\mathbb{Z}_2)$, that is, the 2×2 matrices with entries from the field $\mathbb{Z}_2$.
   (a) How many elements does R have?
   (b) Find all elements that have multiplicative inverses, and list them with their inverses.
5. Consider the ring of *Gaussian integers*, $R = \mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$, where $i^2 = -1$. With the usual addition and multiplication from the complex numbers, it may be shown that R is a ring. Which elements have multiplicative inverses, and what are they?

6. Problem #22.1.3 in Biggs: Show that if x and y are members of a ring R then $(-x)(y) = -(xy)$ and $(-x)(-y) = xy$. At each stage of the proof, explain which property of R you are using. You should not need to assume that multiplication is commutative or that a multiplicative identity 1 exists, though with Biggs's definition of ring you are allowed to assume the existence of a multiplicative identity.

7. Consider the quotient ring $R = \mathbb{Z}_3[x]/\langle q(x)\rangle$ where $q(x) = x^3 + x + 1$. (This polynomial is reducible over $\mathbb{Z}_3$, so R is not a field!)

   How many elements are in R? Compute the products $[2x + 1][x^2]$ and $[x + 2][x^2 + 2x + 2]$ in R.

   Problems due Tuesday, Nov. 2

8. Exhibit an isomorphism between the non-zero elements of $\mathbb{F}_8$ (that is, the multiplicative group of the field) and the elements of $\mathbb{Z}_7$ (considered as an additive group).

9. Use Euclid's gcd algorithm to find the greatest common divisor of $x^3 + 4x^2 + 2x + 2$ and $2x^3 + 4x^2 + 3$ as polynomials in $\mathbb{Z}_5[x]$. (The gcd is a quadratic polynomial.)

10. The polynomial $q = x^2 + 3x + 3$ is irreducible over $\mathbb{Z}_5$ and so can be used to construct the field $\mathbb{F}_{25}$. Use Euclid's algorithm to find the inverse of $\mathrm{p} = [x + 2]$ in $\mathbb{F}_{25}$ by finding polynomials m and n such that $mp + nq = 1$.

11. Consider the quotient ring $R = \mathbb{Z}_5[x]/\langle q(x)\rangle$ where $q(x) = x^2 + 2$. $q(x)$ is irreducible, so this is a field.

    (a) How many elements are in R?

    (b) Find a formula for the multiplicative inverse of the element $[b+ax]$, where $a \neq 0$. (Hint: "Rationalize the denominator." $x = \sqrt{-2}$. To simplify $\frac{1}{[b+ax]}$, multiply numerator and denominator by $[b - ax]$.

    (c) Find the orders of the elements $[x]$ and $[x + 1]$.

12. Biggs, problem 3 on page 317.

13. In the large affine faculty senate two "triangles" are Danny-Gavin-Viola (ABC) and Helen-Sally-Xenia ($A'B'C'$). Show that these six instructors satisfy the conditions and the conclusion of the Desargues axiom.

14. In the medium affine faculty senate, choose the library committee, with Jane as the additive identity. Add Greg and Mike, first using Kate as the auxiliary point, then using Irma. Draw a single diagram representing the addition with both auxiliary instructors, attaching a committee name to each line and an instructor name to each point. Identify the two

"triangles" that are related by Desargues' theorem in the proof that the answer is independent of the choice of instructor.

15. Use the data for the medium affine faculty senate. Choose the library committee, with Jane as the additive identity and Dave as the multiplicative identity. Multiply Greg by Mike, then multiply Mike by Greg, in each case using Kate as the auxiliary point. Draw a single diagram representing the multiplication in both orders, attaching a committee name to each line and an instructor name to each point. Identify the degenerate hexagon of six instructors to which Pappus' Theorem (axiom A5) must be applied to show that the multiplication is commutative.

16. Suppose that A and E are members of a committee of an affine faculty senate whose additive identity is O. Describe a method for constructing the instructor C such that $A + C = E$ using auxiliary instructor B. Prove directly from the axioms that using a different instructor B' on the same committee as O and B leads to the same C. (Of course, this is true for arbitrary B', but the proof becomes tedious). Include a diagram to illustrate how your construction would look in the Euclidean plane, for which your proof is also valid.

17. Choose the quality committee in the large affine faculty senate, with Betty as the additive identity O, Isaac as A, Kevin as C, Yoric as E. Choose James as auxiliary instructor B. Carry out the addition $(A + C) + E$ and $A + (C + E)$, using auxiliary instructors B' and D exactly as described in the notes and in the diagrams on the Web.

    (a) Who is B', and who is D?

    (b) Who is the sum $A + C + E$?

    (c) Redraw the diagram from the Web that shows that addition is associative, with names attached to all the instructors and committees. If two distinct points in the diagram have the same name, don't worry – the diagram is for Euclidean geometry and you are doing finite geometry.

Problems due Tuesday, Nov. 9

18. Suppose that C and E are members of a committee of an affine faculty senate whose additive identity is O and whose multiplicative identity is I. Describe a method for constructing the instructor A such that $AC = E$ using auxiliary member B. Prove directly from the axioms that using a different member B' on the same committee as I and B leads to the same A. (Of course, this is true for arbitrary B', but the proof becomes tedious). Include a diagram to illustrate how your construction would look in the Euclidean plane, for which your proof is also valid.

19. Consider the yearbook committee in the large affine faculty senate. Choose Helen as the additive identity 0 and Sally as the multiplicative identity I. Generate the addition and multiplication tables using affine.exe(downloadable, but for Windows only) or Luke Gustafson's software (from the Web site), and use them to identify the members of the committee with the elements 0, 1, 2, 3, 4 of $\mathbb{Z}_5$.

20. Consider the large affine faculty senate. Choose the housing committee as the x axis and the overseers committee as the y axis. Maria, who serves on both these committees, has coordinates (0,0). Let Wally be the multiplicative identity on the housing committee so that his coordinates are (1,0). Let Emily be the multiplicative identity on the overseers committee so that her coordinates are (0,1). Every instructor now has a coordinate pair (x, y), where x and y are integers mod 5, represented by 0, 1, 2, 3, and 4. The easiest way to find these coordinates for an "axis" committee is to start with the multiplicative identity 1 and keep adding on the multiplicative identity to get 2, 3, and 4. The coordinates of an instructor are found simply by looking at the committees on which that instructor serves that are parallel to the two coordinate axes and taking the values associated with the intersections of these committees with the axes.

    (a) What instructor has coordinates $(1, 2)$?
    (b) What are the coordinates of Betty in this coordinate system?
    (c) What committee satisfies the equation $y = 3x + 2$?
    (d) What equation is satisfied by the diversity committee?

21. Consider the medium affine faculty senate. Choose Greg as the origin. Choose the quality committee as the x-axis, with Lynn as multiplicative identity. Choose the budget committee as y-axis, with Emma as multiplicative identity. The finite field $\mathbb{F}_4$ has elements $[0], [1], [u], [u + 1]$, where $[u][u + 1] = [1]$, and all arithmetic is carried out modulo 2; i.e. $[1]+[1] = [0]$.

    (a) . What instructor has coordinates ([1],[1])? What committee satisfies the equation $y = x$? Assign coordinates $([u], [u])$ to whichever remaining instructor on this committee is first alphabetically.
    (b) Determine the coordinates of all the instructors. Show your answer on a diagram, with the x axis horizontal and the y axis vertical.
    (c) Which committee satisfies $y = [u]x$, and which satisfies $y = [u+1]x$?
    (d) What equation is satisfied by the insurance committee?
    (e) What committee satisfies the equation $x + [u]y = [u + 1]$?

22. A collineation of an affine faculty senate is a bijection f that maps instructors to instructors and committees into committees in such a way that

- If instructors A and B serve on committee s, then $f(A)$ and $f(B)$ both serve on $f(s)$.
- If committees s and t intersect in instructor A (or are parallel), then $f(s)$ and $f(t)$ intersect in $f(A)$ (or are parallel).

For the small affine faculty senate, any collineation that fixes three points (instructors) is the identity and every collineation is an affine transformation, a linear transformation (represented by a matrix A) followed by a translation (addition of a vector $\vec{b}$).

(a) Find the unique collineation that maps Bob into Ian, Hal into Cal, and Gus into Amy. Make a table showing the image of each instructor and each committee.

(b) Find a matrix A and vector $\vec{b}$ that represents this mapping in a coordinate system where Bob is (0,0), Hal is (1,0), and Gus is (0,1). The entries in the matrix and vector will be integers modulo 3, so they will all be 0, 1, or 2.

23. For the medium affine senate, there are collineations that hold three points (instructors) fixed but that are not the identity. Find such a collineation that holds Dave, Jane, and Owen fixed. Make a table showing the image of each instructor and each committee. Since the square of this collineation is the identity, it either holds a given committee or instructor fixed or interchanges two committees or instructors; so your table only has to show the instructors and committees that get interchanged.
Hint: Choose one instructor (say Dave) as the additive identity for both axes, the other two (Jane and Owen) as the multiplicative identities for the two axes. Find the instructor whose coordinates are (1,1). Now you have an arbitrary choice about who on the committee containing (0,0) and (1,1) has coordinates (u, u) and who has $(u+1, u+1)$. Interchanging these two instructors leads to the desired collineation.

Problems due Tuesday, Nov. 16

24. In a vector space there are two "zeroes", the additive identity for the field F, 0, and the zero vector, $\vec{0}$.

(a) Justify the statement that 0+0=0 in the field F, Then, by applying vector space axioms to $(0 + 0)\vec{v} = 0\vec{v}$, prove that for any vector $\vec{v}$, $0\vec{v} = \vec{0}$.

(b) Invent a similar proof that for any a in the field F, $a\vec{0} = \vec{0}$.

(c) -1 is the additive inverse of the multiplicative identity in F, while $-\vec{v}$ is the additive inverse of $\vec{v}$. Prove that for any vector $\vec{v}$, $(-1)\vec{v} = -\vec{v}$.

25. Prove by brute force the Cayley-Hamilton theorem for 2×2 matrices: a matrix A satisfies its own characteristic equation, or
$A^2 - (trA)A + (detA)I = 0$.

26. How many matrices are in the group $GL(3, \mathbb{Z}_3)$ and how many in $SL(3, \mathbb{Z}_3)$? In each case, how many of the matrices are diagonal?

27. Consider the matrix $\left[\begin{smallmatrix} 1 & 0 \\ 3 & 1 \end{smallmatrix}\right]$ from $SL(2, \mathbb{Z}_5)$. Let this matrix act five times in succession, starting with the vector $\left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right]$, and thereby verify that it permutes the five vectors of the form $\left[\begin{smallmatrix} 1 \\ y \end{smallmatrix}\right]$.

28. Consider the matrix $A = \left[\begin{smallmatrix} 3 & 3 \\ 2 & 3 \end{smallmatrix}\right] \in GL_2(\mathbb{Z}_5)$.

(a) Find the eigenvalues of A.

(b) Assuming that A acts on the vector space $V = (\mathbb{Z}_5)^2$, find an eigenvector for each eigenvalue you found in (a).

29. Use the Cayley-Hamilton theorem to show that in $SL(2, \mathbb{F}_4)$

(a) a matrix A with trace 0 has order 2

(b) a matrix A with trace 1 has order 3

(c) a matrix A with trace x has order 5

Exploratory Problems

1. Prove by induction that if a vector space V is spanned by n vectors $\vec{v_1}$, $\vec{v_2}...\vec{v_n}$, any set of $n+1$ vectors $\vec{w_1}$, $\vec{w_2}$,...$\vec{w_{n+1}}$ in V must be linearly dependent. The base case $n = 1$ was done in class, as was a proof for the case $n = 2$ that illustrates how to do the inductive step.

2. In this exercise, we consider the group A_4 and its normal subgroup V_4, the Klein Four group, and show that the quotient group A_4/V_4 is isomorphic to C_3.

Exhibit V_4 as a (normal) subgroup of the rotation group of the tetrahedron. List as permutations the members of the three cosets. Identify each coset with an element of C_3. For each pair of cosets (recall that C_3 is abelian!), perform the multiplication by members of the cosets chosen at random, and thereby reconstruct the multiplication table for C_3.

3. Consider the ring $R = F[x]$, where F is a field. Suppose $a(x), b(x) \in R$ are non-zero. Show that $deg(a(x)b(x)) = deg(a(x)) + deg(b(x))$. Construct a counterexample to show that this result is not always true in the ring $\mathbb{Z}_6[x]$.

4. Biggs, problem 5 on page 322.

   The next two problems refer to Bennett, Affine and Projective Geometry, on reserve on Cabot Library or in the Birkhoff Math Library on the 3rd floor of the Science Center (use Hollis to get the call number – there is no card in the card catalog).

5. Bennett, problem 7 on page 55.

6. Consider the kitchen committee in the large affine senate, with Alice as additive identity O and Ralph as multiplicative identity I. Let James be point A in Figure 3.20 on p. 67 of Bennett; let Nancy be C and Viola E. Choose Xenia as the auxiliary instructor B. Redraw Figure 3.20 from Bennett (for the proof of the distributive law $(A + C)E = AE + CE$), attaching an instructor name to each point and a committee name to every line.

7. Let G be the group of symmetries of the cube. (Recall that $|G| = 24$.) By orienting the the cube in $\mathbb{R}^3$ with its vertices at the eight points $(\pm 1, \pm 1, \pm 1)$, write down the 3×3 matrices that represent these symmetries.

   Check your work by verifying that the numbers of matrices of orders 1,2,3, and 4 are 1,6,8, and 9, respectively. What are the eigenvalues for one matrix of each type, and what are the multiplicities?

8. Let $A \in M_n(F)$. Recall that the *characteristic polynomial* of A is $f_A(\lambda) = \det(A - \lambda I)$, and that λ is an eigenvalue of A if and only if $f_A(\lambda) = 0$.

   Define the *algebraic multiplicity* of the eigenvalue λ_0 to be the number of times λ_0 was a root of the characteristic polynomial. (That is, if k is the algebraic multiplicity, we may write $f_A(\lambda) = (\lambda - \lambda_0)^k \cdot g(\lambda)$, where $g(\lambda_0) \neq 0$.) Define the *geometric multiplicity* of λ_0 to be the dimension of its corresponding eigenspace, $dim(E_{\lambda_0})$.

   Show that the algebraic multiplicity of an eigenvalue is always greater than or equal to its geometric multiplicity.

9. Conway's atlas of groups claims that $SL(3, \mathbb{Z}_2)$ has 168 elements, some of which are of order 7. Confirm the number of elements, find one element whose order is 7, and compute its powers.

10. (This is pasted in by hand because of the complicated diagram; so it will not appear in the Web version of this document You can download it as the file Hessenberg.rtf.)

11. (This is the second problem on the same page as the previous problem.)