MATHEMATICS 152, FALL 2003
METHODS OF DISCRETE MATHEMATICS
Outline #6 (Rings and Fields, especially Finite Fields)

None of this material is needed for the half-hour quiz on Oct. 9, which will cover outlines 1 through 5 and the first three homework assignments.

We define rings and fields, provide basic examples, construct more complex examples, and study the structure of these objects.

1. Define a *ring* as a set with two binary operations, traditionally denoted + and ·, satisfying a set of axioms that Biggs summarizes as R1, R2, and R3. Expand R1 into A1-A5, R2 into M1-M2, and call R3 D. A ring which satisfies M3 is said to be a *ring with identity*;Axioms M5 and M4 are the "extra algebraic properties that Biggs mentions at the top of p. 197. A ring which also satisfies M4 is said to be a *division ring*; and a ring which also satisfies M5 is said to be a *commutative ring*. A ring that satisfies all eleven axioms is said to be a *field*.

   Write out all the axioms explicitly. Then, by considering (1+1)(a+b) and using the distributive law, prove that, for the case of a field, the axiom that addition is commutative (you probably called it A5) follows from the other axioms. (Sections 22.1–22.3.)

2. Show that the following examples satisfy the axioms above:

   (a) the integers, $\mathbb{Z}$, which form a commutative ring with identity,

   (b) the congruence classes of integers modulo n, denoted $\mathbb{Z}_n$, which form a commutative ring with identity in all cases and a field when n is prime,

   (c) the polynomials with real coefficients, denoted $\mathbb{R}[x]$, which form a commutative ring with identity.

   (d) the $n \times n$ matrices with real entries, denoted $M_n(\mathbb{R})$, which form a ring with identity (and a field in the special case $n = 1$).

   (Sections 22.1, 22.3, and 22.4.)

3. Consider the more abstract rings of polynomials, $F[x]$, where F is any field. (In particular, we are interested in the case where $F = \mathbb{Z}_p$ for a prime p.) State the Division Algorithm and the Euclidean Algorithm for polynomial rings. (Sections 22.4–22.6.)

4. Construct the equivalence classes of polynomials modulo $q(x)$, for a specified polynomial $q(x)$ of degree n. How many such equivalence classes are there when $F = \mathbb{Z}_p$? Define addition and multiplication on the set of equivalence classes by $[a(x)] + [b(x)] = [a(x) + b(x)]$ and $[a(x)][b(x)] = [a(x)b(x)]$, and show that with these definitions, the set of equivalence classes forms another ring, known as a *quotient ring*. (Sections 23.1 and 23.3.)

5. In the construction above, show that the quotient ring is in fact a field when $q(x)$ is *irreducible*. Give examples of irreducible polynomials of degree 2 and 3 in the polynomial rings $F[x]$ when $F = \mathbb{Z}_2$, $\mathbb{Z}_3$, and $\mathbb{Z}_5$. (Pay special attention to the case $p = 3$ and $q(x) = x^2 + 1.$, done in Biggs section 23.1) (Sections 22.7–22.8 and 23.3.)

6. For the case where $p = 2$ and $q(x) = x^2 + x + 1$, the four elements of the field are [0],[1], $[x]$, and $[x + 1]$. Show how to build up the multiplication table for this field of four elements, $\mathbb{F}_4$, by using the rules that

   - All coefficients are in $\mathbb{Z}_2$ so that $1 + 1 = 0$.
   - $x^2 + x + 1 = 0$ so that x^2 can always be replaced by $x + 1$.

   (See Exercise 23.2 in Biggs)

7. By counting the number of distinct products of non-zero monic linear polynomials with coefficients in $\mathbb{Z}_p$ and the number of non-zero monic quadratic polynomicals with coefficients in $\mathbb{Z}_p$, prove that there exists at least one irreducible monic quadratic polynomial for any prime p (Section 22.8).

8. For the field $\mathbb{F}_9$ with irreducible polynomial $x^2 + 2x + 2$ (note – this is not the same polynomial that Biggs uses in section 23.1) make a table of all the powers of $[x]$.Show how to use this result to find the inverse of any nonzero element and to do multiplication by means of addition. (This is the finite case of logarithms!)(Section 23.4)