MATHEMATICS 152, FALL 2004
METHODS OF DISCRETE MATHEMATICS
Outline #6 (Rings and Fields, especially Finite Fields)

Last modified: September 12, 2004

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

1. Define a *ring with identity* as a set with two binary operations, traditionally denoted + and $\cdot$, satisfying a set of axioms that Biggs summarizes as R1, R2, and R3. Expand R1 into A1-A5, R2 into M1-M3, and call R3 D. Axioms M5 and M4 are the "extra algebraic properties" that Biggs mentions at the top of p. 297. 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*.

   Show that the integers $\mathbb{Z}$ form a commutative ring with identity. Show that the even integers $2\mathbb{Z}$ satisfy all the axioms except M3 and M4 and thus form a commutative ring without identity. According to the definition in Biggs, this is not a ring. Most authors would disagree, but we will never have occasion to consider rings that without identity and can therefore safely use the term "ring," as Biggs does, to mean "ring with identity" (Sections 22.1–22.3.)

2. A number of laws of arithmetic that you have known for a long time are surprisingly absent from the list of axioms for a field.

   (a) $0a = 0$

   (b) $(-1)a = -a$

   (c) $(-a)(-b) = ab$

   In fact, they are all easily-proved theorems that follow from the distributive law and the axiom that every element has an additive inverse.

   (a) By considering $(0 + 0)a$ and using the distributive law, prove that $0a = 0$ for every element a of a field.

   (b) Now consider $(1 + (-1))a$ and prove that $(-1)a = -a$. Setting $a = -1$, prove that (-1)(-1)=1.

   (c) Finally, use the associative and commutative laws to prove that $(-a)(-b) = ab$.

   (It is true even for a non-commutative ring without identity that $(-a)(-b) = ab$, but this more tedious proof is left for the homework.)

3. 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 (which was probably called A5 in the preceding topic) follows from the other axioms.

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

   (a) 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,

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

   (c) 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.)

5. 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, but do not present the rather tedious proofs. (Sections 22.4–22.6.)

6. Consider 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.)

7. 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.)

8. 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)

9. Review how the field of complex numbers $\mathbb{C}$ is built as an extension of the field of real numbers $\mathbb{R}$ by introducing a symbol i that denotes a solution to the equation $i^2 + 1 = 0$, which has no solution in the field of real numbers. Show how this equation is used to define multiplication in the field of complex numbers; for example, in calculating $(2 + i)(3 + 2i)$. Explain why there is really no way to say what is i and what is $-i$, and contrast this situation with what happens when you extend the field $\mathbb{Q}$ of rational numbers by introducing a positive number y (usually denoted $\sqrt{2}$) that satisfies $y^2 - 2 = 0$.

10. As an alternative but equivalent way of constructing the field $\mathbb{F}_4$ as an extension of the field $\mathbb{Z}_2$, introduce a symbol x that denotes a solution to the equation $x^2 + x + 1 = 0$, which has no solution in the field $\mathbb{Z}_2$. Show how this equation satisfied by x is used to define multiplication in the field $\mathbb{F}_4$; for example, in calculating $(x + 1)(x)$. Explain why there is really no way to say what is x and what is $x + 1$.

11. 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 polynomials with coefficients in $\mathbb{Z}_p$, prove that there exists at least one irreducible monic quadratic polynomial for any prime p (Section 22.8).

12. 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. Building a table like this leads to the simplest way of implementing finite fields in software, as in the second programming project. (Section 23.4)