189-235A: Basic Algebra I
Assignment 6
Due: Wednesday, November 9, 2005

1. For which odd primes $p \leq 23$ is the polynomial x^2+1 irreducible in $\mathbf{Z}_p[x]$? Can you detect a pattern?

2. Find a polynomial of degree 2 in $\mathbf{Z}_6[x]$ that has four roots in $\mathbf{Z}_6$. Why does this not contradict the theorem shown in class that a polynomial in $F[x]$ of degree d has at most d roots?

3. Find the inverse of $[x^2+x+1]$ in the ring $\mathbf{Z}_2[x]/(x^3+x+1)$.

4. Write down all the powers of $[x]$ in the finite ring $\mathbf{Z}_2[x]/(x^3+x+1)$. What is the smallest $j > 1$ such that $[x]^j = 1$?

5. If p is an odd prime of the form $3+4m$, show that the polynomial x^2+1 is irreducible in $\mathbf{Z}_p[x]$, so that $\mathbf{Z}_p[x]/(x^2+1)$ is a field.

6. Which of the following subsets I of a commutative ring R are ideals of R? Justify your answer.

6a. $R = F[X]$, where F is a field, and $I = F$ is the set of constant polynomials.

6b. $R = \mathbf{Z} \times \mathbf{Z}$, and $I = \{(m, 0) \quad \text{where } m \in \mathbf{Z}\}$.

6c. The set of *nilpotent elements* of a ring R, i.e., those $a \in R$ such that $a^n = 0$ for some n.

6d. R is the ring of functions from $\mathbf{Z}$ to the real numbers $\mathbf{R}$, and I the subset of those functions f satisfying $f(0) = f(1)$.

6e. R is the ring of functions from $\mathbf{Z}$ to $\mathbf{R}$, and I the subset of those functions

f satisfying $f(0) = f(1) = 0$.

7. Let R be the polynomial ring $F[x]$ with coefficients in a field. Adapt the argument given in class for $R = \mathbf{Z}$ to show that every ideal of R is principal.

Extra credit problems

Let $\mathbf{Q}(\sqrt{-5}) = \{a + b\sqrt{-5}, a, b \in \mathbf{Q}\}$, and $\mathbf{Z}[\sqrt{-5}] = \{a + b\sqrt{-5}, a, b \in \mathbf{Z}\}$.

8. Show that $\mathbf{Q}(\sqrt{-5})$ is a field, and that $\mathbf{Z}[\sqrt{-5}]$ is a subring. It is called the *ring of integers* of $\mathbf{Q}(\sqrt{-5})$ and plays the role of the usual integers in the arithmetic of $\mathbf{Q}(\sqrt{-5})$.

9. Show that the invertible elements in $\mathbf{Z}[\sqrt{-5}]$ are exactly 1 and -1.

10. Show that the elements 2, 3, $1+\sqrt{-5}$ and $1-\sqrt{-5}$ are irreducible. (I.e., they cannot be written in the form ab where $a, b \neq \pm 1$.)

11. Using 9, show that the ring $\mathbf{Z}[\sqrt{-5}]$ is not a unique factorization ring. (I.e., the "integers" in $\mathbf{Z}[\sqrt{-5}]$ cannot be written uniquely as a product of irreducible elements.)

12. Show that the ideals $(2, 1+\sqrt{-5})$, $(3, 1+\sqrt{-5})$, and $(3, 1-\sqrt{-5})$ are not principal, and that they are *irreducible*, i.e.,they cannot be factored further into products of non-trivial ideals.

13. If I and J are ideals, define the product IJ to be the ideal generated by the elements of the form ij with $i \in I$ and $j \in J$. Show that $(2, 1 + \sqrt{5})^2 = (2)$, $(3, 1+\sqrt{-5})(3, 1-\sqrt{-5}) = (3)$, and conclude that the ideal (6) factorizes as a product of 4 (non-principal) ideals: $(6) = (2, 1+\sqrt{-5})^2(3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$.

Remark: It can be shown that this factorization of the principal ideal (6) into a product of irreducible ideals is *unique*, up to the order of the factors. This is a general phenomenon: although the ring $\mathbf{Z}[\sqrt{-5}]$ fails to satisfy unique factorization, its *ideals* can be expressed uniquely as products of irreducible ideals. The introduction of ideals in the late 19-*th* century by Dedekind was an attempt to salvage unique factorization in such rings, by showing it was true on the level of ideals which were viewed as a kind of “ideal number”. This is where the terminology comes from...