Abstract Algebra 2 **Spring 2007** **Solutions to HW #1**

1. (16, #12) This was straight forward.

2. (16, #24) This I essentially did in class.

3. (17, # 6) Let $f(x) \in Z_p[x]$ be ireducible of degree n. Prove that $Z_p[x]/(f(x))$ is a field with p^n elements (I am going to use ( ) instead of $\langle\ \rangle$).

   Proof: Since $f(x)$ is irreducible and since $Z_p[x]$ is a PID, $(f(x))$ is a maximal ideal. In particular $Z_p[x]/(f(x))$ is a field.

   Also $E := Z_p[x]/(f(x))$ is a vector space over Z_p. Hence its order is p^k where k is the dimension of E over Z_p. It suffices to show that if a is the image of x in E, then $1, a, a^2, \ldots, a^{n-1}$ is a basis for E (over Z_p).

   Linear independence: Suppose that

   $$b_n a^n + b_{n-1}a^{n-1} + \ldots + b_0 = 0,$$

   where $b_i \in Z_p$. Thus $b_n x^n + b_{n-1}x^{n-1} + \ldots + b_0$ (viewed as an element of $Z_p[x]$) must be in the ideal $(f(x))$. Which means that it is divisible by $f(x)$. However, it has degree less than n, so this must be the zero polynomial. Hence $b_n = b_{n-1} = \ldots b_0 = 0$. Spans:

   An arbitrary element of E is a coset of the form $g(x) + (f(x))$ for some polynomial $g(x)$. Suppose that $f(x) = x^n + \ldots + a_0$, (we can assume that f is monic). Then $x^n + (f(x)) = -a_{n-1}x^{n-1} - \ldots - a_0 + (f(x))$. In this fashion, all higher powers of x can be reduced modulo the ideal $(f(x))$ to something in powers of less than n. So the cosets $1, x + (f(x)), \ldots$ span. But these are the elements $1, a, a^2, \ldots$

4. (17, # 18) Prove that for any positive integer n, there are infinitely many polynomials of degree n in $Z[x]$ that are irreducible over $\mathbb{Q}$.

   Proof: This is one line. For each prime number p, $x^n - p$ is irreducible over $\mathbb{Q}$ by Eisenstein. Since there are infinitely many choices for p, we're done.

5. (17, #32) Prove that the ideal $(x^2 + 1)$ is a prime of $Z[x]$, but not a maximal ideal.

   Proof: Clearly x^2+1 is an irreducible element of $Z[x]$. Since $Z[x]$ is a UFD, it is a prime element of $Z[x]$. Thus $(x^2 + 1)$ is a prime ideal. To show that it is not a maximal ideal, it suffices to show that it is properly contained in an other ideal. Let $I = (x^2 + 1, 2)$.

Clearly $(x^2+1) \subseteq I$. Moreover $2 \in I$, yet 2 is clearly not a multiple of x^2+1 (look at degree). Thus I is strictly bigger than (x^2+1). Also note that I is the kernel of the map from $Z[x]$ to Z_2 given by $f \mapsto f(2)$. Thus I is a proper ideal.

6. (18, # 28) Determine the units of $R := Z[i]$.

We know that $Z[i] = \{a+bi : a, b \in Z\}$. Let $u = a+bi$ be a unit of R. Thus there exists an element $c+di$ such that $(a+bi)(c+di) = 1$. Also $(a+bi)(c+di) = (ac-bd)+(bc+ad)i$. Hence we have

$$\begin{aligned} ac - bd &= 1 \\ bc + ad &= 0 \end{aligned}$$

Add a times the first row to b times the second row to get $a^2c+b^2c = a$ or $(a^2+b^2)c = a$. From this we get

$$c = \frac{a}{a^2+b^2}$$

Since c (as well as a and b) are integers, it follows that $b = 0$ or $a = 0$, but not both, otherwise $u = a+bi = 0$. If $b = 0$, Then since c is an integer, $a = \pm 1$. Since $b = 0$, we have $u = \pm 1$.

Now suppose that $a = 0$. Then from the second of the array, we have $bc = c$. Hence $c = 0$. Thus $(a+bi)(c+di) = bci^2 = -bc = 1$. Thus $b = \pm 1$. Hence $u = \pm i$.