Math 100b Winter 2010 Homework 2

Due 1/22/09 in class

Reading

All references will be to Beachy and Blair, 3rd edition.

Read sections 5.2 and 5.3, and catch up on any earlier reading (5.1, 4.1, 4.2.)

Extra Problems

These are generally easier or just extra problems you should look over to check your understanding of the material. They are not to be handed in.

Section 4.1: 1, 2, 5, 6

Section 4.2: 1(a)(c)

Section 5.2: 1, 3, 4, 5, 8, 9.

Assigned Problems

Write up neat solutions to these problems.

Section 4.2: 1(d), 2(b)

Section 5.2: 2, 7 (an automorphism is just an isomorphism from a ring to the same ring), 15

Additional Problems

1. Let p be prime, and consider the polynomial $f(x) = x^{p-1} - 1$ in the ring $\mathbb{Z}_p[x]$. (If one wanted to be notationally more formal, this would be written as $[1]_p x^{p-1} - [1]_p$, but I think you should omit brackets now and just remember that all operations on coefficients are done modulo p).

(a) Find all roots of $f(x)$ in $\mathbb{Z}_p$.

(b) Factor $f(x)$ completely as a product of irreducible polynomials in $\mathbb{Z}_p[x]$. (Hint: factor theorem.)

(c) By comparing the constant term of $f(x)$ with the constant term of its factorization into irreducibles in (b), give another proof of Wilson's theorem (Exercise 27 in section 1.4, page 44 of the text.)

2. In the ring $\mathbb{R}[x]$, find the remainder when $x^{20} - 2x^{19} + 5x - 7$ is divided by $(x - 2)$, without actually performing the polynomial division.

3. Let F be a field and let $g(x) \in F[x]$ be a polynomial of degree $n \geq 1$. Consider the factor ring $R = F[x]/\langle g(x)\rangle$.

(a) An arbitrary element of R is a coset $f(x) + \langle g(x)\rangle$, where $f(x)$ is any polynomial. Show that given such a coset there is a *unique* polynomial $r(x)$ with $\deg r < n$ and such that $f(x) + \langle g(x)\rangle = r(x) + \langle g(x)\rangle$.

(Remark: This result is very useful, because it shows that in writing down the cosets $r(x)+\langle g(x)\rangle$ for all r with $\deg r < n$ we list all of the elements of R without repeats. In other words, the set $\{r(x)|\deg r < n\}$ contains exactly one element from each distinct coset of $\langle g(x)\rangle$. This is analogous to the way that the set $\{0, 1, \ldots, n-1\}$ contains exactly one element from each distinct coset of $n\mathbb{Z}$ in $\mathbb{Z}$.)

(b). Take $F = \mathbb{Z}_p$ for some prime p, and use the result of part (a) to count the number of elements in $\mathbb{Z}_p[x]/\langle g(x)\rangle$ where again $\deg g = n$.

(c). Using part (b), show that $R = \mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle$ is a ring with four elements. Write down those four elements using the unique coset representatives of smallest degree as in part (a). Find explicitly the 4×4 multiplication table of R and prove in this way that R is a field.

(Remark: This field of 4 elements is an entirely new ring we have never seen. Fields with finitely many elements are extremely important and have many applications. While the factor ring $\mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle$ may seem to you a complicated way to describe such a field, taking factor rings of polynomial rings is actually the easiest way to discover such fields. In part (c), there is a less calculation-oriented way of proving that R is a field, which we may cover in class prior to your handing in this homework. I want you to write down the multiplication table and do it that way in any case, because actually getting your hands dirty with a calculating products in a factor ring is important for you to do at this point.)

4. Let d be a positive integer which is not a perfect square (take as given the well-known fact that $\sqrt{d}$ is an irrational number.) Consider the ring $\mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} | a, b \in \mathbb{Q}\}$, as a subring of $\mathbb{R}$, which you proved on the preceding homework is a field.

Show that $\mathbb{Q}[x]/\langle x^2 - d\rangle \cong \mathbb{Q}[\sqrt{d}]$.