Math 4000/6000 – Homework #8

posted November 9, 2015; due at the **start of class** on November 16, 2015

> Some mathematics problems look simple, and you try them for a year or so, and then you try them for a hundred years, and it turns out that they're extremely hard to solve. There's no reason why these problems shouldn't be easy, and yet they turn out to be extremely intricate. – Andrew Wiles

Assignments are expected to be neat and stapled. **Illegible work may not be marked**. Starred problems (*) are required for those in MATH 6000 and extra credit for those in MATH 4000.

0. (Work but do not turn in)

   (a) Prove that if F is a field and $f(x) \in F[x]$ has degree $n \geq 1$, then the elements of $F[x]/\langle f(x)\rangle$ all have the form $a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$, where $a_0, \ldots, a_{n-1} \in F$. Moreover, show that this representation is unique; i.e., distinct choices of a_i lead to distinct elements of $F[x]/\langle f(x)\rangle$.

   Hint: This is closely related to Problem #6 on HW #7.

   (b) Suppose that $\phi\colon R \to S$ is a ring homomorphism. Let B be the image of ϕ, i.e., $B = \{\phi(r) : r \in R\}$. Prove that B contains 1_S, is closed under the $+$ and $\cdot$ from S, and is closed under additive inverses. (It then follows from results on earlier homework that B is a subring of S.)

1. Let R be a commutative ring. If I and J are two ideals of R, define

$$I + J = \{a + b : a \in I, b \in J\}.$$

   Show that $I + J$ is an ideal of R and that $I + J$ contains both I and J.

2. Exercise 4.1.3.

   Note: In part (c), assume that R is not the zero ring.

3. Let m be a positive integer. In this problem, we work in the ring $\mathbb{Z}_m$.

   (a) Show that every ideal of $\mathbb{Z}_m$ is principal.

   Hint: Given an ideal I of $\mathbb{Z}_m$, show that $I = \langle\bar{a}\rangle$ if a is chosen as the smallest positive integer with $\bar{a} \in I$.

   (b) Show that if a and b are integers, then $\langle\bar{a}\rangle = \langle\bar{b}\rangle$ in $\mathbb{Z}_m$ if and only if $\gcd(a, m) = \gcd(b, m)$.

   (c) How many distinct ideals of $\mathbb{Z}_{11}$ are there? of $\mathbb{Z}_{30}$?

4. (a) (Isomorphism is symmetric) Suppose $\phi\colon R \to S$ is an isomorphism. Since ϕ is a bijection, it has an inverse; in other words, there is a map $\psi\colon S \to R$ satisfying

$$(\psi \circ \phi)(r) = r \text{ for all } r \in R, \quad (\phi \circ \psi)(s) = s \text{ for all } s \in S.$$

   Prove that ψ is an isomorphism from S to R.

   Hint: You may assume as known that ψ is a bijection.

(b) (Isomorphism is transitive) Suppose $\phi\colon R \to S$ and $\psi\colon S \to T$ are isomorphisms. Prove that $\psi \circ \phi$ is an isomorphism from R to T.

Hint: You may assume as known that the composition of bijections is a bijection.

5. Exercise 4.2.1.

6. Use the Fundamental Homomorphism Theorem to establish the following ring isomorphisms.

   (a) $\mathbb{R}[x]/\langle x^2 + 6\rangle \cong \mathbb{C}$.

   (b) $R[x]/\langle x\rangle \cong R$ for every commutative ring R.

   (c) $\mathbb{Z}_{18}/\langle \bar{6}\rangle \cong \mathbb{Z}_6$.

   (d) $\mathbb{Q}[x]/\langle x^2 - 1\rangle \cong \mathbb{Q} \times \mathbb{Q}$.

   Hint: Consider the homomorphism from $\mathbb{Q}[x]$ to $\mathbb{Q}\times\mathbb{Q}$ given by $f(x) \mapsto (f(1), f(-1))$.

7. Exercise 4.2.12.

8. Exercise 4.2.13.

9. (Existence of finite fields of size p^n) Let p be a prime and let n be a positive integer. Consider the polynomial $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$. Let $K/\mathbb{Z}_p$ be a field extension in which f splits. So in $K[x]$, we may write

$$f(x) = (x - \alpha_1)\cdots(x - \alpha_{p^n}).$$

   (We proved in class that such a field K exists.) Let F be the set of roots, i.e., $F = \{\alpha_1, \ldots, \alpha_{p^n}\}$.

   (a) Show that all of the α_i are *distinct*. Thus, F has size p^n.

   Hint: Use Exercise 3.1.15 (which was on previous HW) to rule out f having a multiple root.

   (b) Show that F is a subring of K.

   (c) Show that F is in fact a subfield of K.

   Hint: Every nonzero $\alpha \in F$ certainly has an inverse in K, since K is a field. You must check that this inverse belongs to F.

10. (*) Let m and n be positive integers. Show that if $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$, then $\gcd(m, n) = 1$. (This is the converse of an assertion proved in class.)

11. (*) We call a nonzero polynomial $f(x) \in \mathbb{Z}[x]$ **primitive** if there is no prime dividing all of its coefficients. For example, $2x + 1$, $7x^2 - 3$, and $x^2 + 2x + 4$ are primitive, but 2 and $3x^2 + 3$ are not.

    (a) Let $f(x)$ and $g(x)$ be polynomials in $\mathbb{Z}[x]$. Suppose that $f(x)$ divides $g(x)$ in $\mathbb{Q}[x]$, and that $f(x)$ is primitive. Show that $f(x)$ divides $g(x)$ in $\mathbb{Z}[x]$.

    Hint: Imitate the proof of Gauss's lemma.

(b) Using the result of (a) and the fundamental ring homomorphism theorem, show that

$$\mathbb{Z}[x]/\langle x^2+1\rangle \cong \mathbb{Z}[i].$$

Hint: Consider the map ϕ from $\mathbb{Z}[x]$ to $\mathbb{Z}[i]$ sending $f(x)$ to $f(i)$. Use (a) to prove that the kernel of this map is $\langle x^2+1\rangle$.

(c) Using the result of (a) and the fundamental ring homomorphism theorem, show that

$$\mathbb{Z}[x]/\langle 2x-1\rangle \cong \left\{\frac{r}{s} : r, s \in \mathbb{Z}, s = 2^j \text{ for some integer } j \geq 0\right\}.$$

(You may assume the straightforward-to-verify fact that the right-hand side is a subring of $\mathbb{Q}$.)