Math 4000/6000 – Homework #7

posted April 10, 2018; due at the **start of class** on April 18, 2018

> Many who have never had occasion to learn what mathematics is confuse it with arithmetic, and consider it a dry and arid science. In reality, however, it is the science which demands the utmost imagination.
> – Sofia Kovalevskaya (1850–1891)

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.

1. Prove the following proposition stated in class: If F is a field and $f(x) \in F[x]$ has degree $n \geq 1$, then the elements of $F[x]/f(x)F[x]$ all have the form $\overline{a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}}$, 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 for the first half: For any $a(x) \in F[x]$, we can write $a(x) = f(x)q(x) + r(x)$, where $r(x) = 0$ or $\deg r(x) < n$. Argue that $\overline{a(x)} = \overline{r(x)}$.

2. Let F be a field and let $p(x)$ be an irreducible polynomial in $F[x]$. Prove that $F[x]/p(x)F[x]$ is a field.

   Hint: Imitate our earlier proof that $\mathbb{Z}_p$ is a field when p is a prime. Namely, suppose $\overline{a(x)}$ is not $\overline{0}$ in $F[x]/p(x)F[x]$. Then $p(x)$ does not divide $a(x)$. What does this mean about $\gcd(p(x), a(x))$? Go from there.

3. Let F be a subfield of K. Let $\alpha \in K$.

   (a) Let $I = \{f(x) \in F[x] : f(\alpha) = 0\}$. Show that I is an ideal of $F[x]$.

   (b) Suppose that there is an irreducible polynomial $p(x) \in F[x]$ with $p(\alpha) = 0$. Show that then $I = p(x)F[x]$, where I has the same meaning as in part (a).

4. Let R be a commutative ring, and let I be an ideal of R. Prove that R/I is the zero ring if and only if $I = R$.

5. Let R be a commutative ring, not the zero ring. We say that an ideal $I \subseteq R$ is a **prime ideal** if

   (i) $I \neq R$,

   (ii) whenever a and b are elements of R for which $ab \in I$, either $a \in I$ or $b \in I$ (or both).

   Show that for every ideal I of R,

   $$R/I \text{ is a domain} \iff I \text{ is a prime ideal of } R.$$

6. Find, with proof, all of the prime ideals of $\mathbb{Z}$.

7. (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

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

   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 take as known that the composition of bijections is a bijection.

8. Let $\phi\colon R \to S$ be an isomorphism of rings.

   (a) Give a detailed proof that r is a zero divisor in $R \Longleftrightarrow \phi(r)$ is a zero divisor in S.

   (b) Give a detailed proof that r is a unit in $R \Longleftrightarrow \phi(r)$ is a unit in S.

9. Exercise 4.2.1.

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

    (a) $\mathbb{R}[x]/\langle x^2 + 6\rangle \cong \mathbb{C}$.
    Hint: Consider the "evaluation at $i\sqrt{6}$" homomorphism taking $f(x) \in \mathbb{R}[x]$ to $f(i\sqrt{6}) \in \mathbb{C}$.

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

    (c) $\mathbb{Q}[x]/\langle x^2 - 1\rangle \cong \mathbb{Q} \times \mathbb{Q}$. *Hint:* Consider the homomorphism from $\mathbb{Q}[x]$ to $\mathbb{Q} \times \mathbb{Q}$ given by $f(x) \mapsto (f(1), f(-1))$.

11. (*) 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 we will prove in class.)

    Hint: Look at the number of times you have to add an element to itself to return to 0.

12. (*) Exercise 3.3.7.