Mathematics 103B Practice problems
Exam 2

1. Let \( f(x) = x^4 + 4x + 5 \) and \( g(x) = x^2 + 2x + 2 \) be polynomials in \( \mathbb{Z}/7\mathbb{Z}[x] \). Find the quotient and remainder for dividing \( f(x) \) by \( g(x) \).

   \[ f(x) = (x^2 - 2x + 2)(x^2 + 2x + 2) + 4x + 1. \]

   Thus the quotient is \( x^2 - 2x + 2 \) and the remainder is \( 4x + 1 \).

2. Give an explicit example of an infinite field of characteristic 7. Is there an example of an infinite field of characteristic 6?

   One such example is \( \mathbb{Z}/7\mathbb{Z}(x) \), the field of fraction of \( \mathbb{Z}/7\mathbb{Z}[x] \).

   There is no infinite field of characteristic 6, because the characteristic of any integral domain is 0 or prime.

3. Let \( \mathbb{Z}[x, y] = \mathbb{Z}[x][y] \) be the polynomials in the two variables \( x, y \) with integer coefficients. Is there a field that contains \( \mathbb{Z}[x, y] \)? How about \( \mathbb{Z}/6\mathbb{Z}[x, y] \); is there a field that contains this ring?

   The ring \( \mathbb{Z}/6[x, y] \) cannot be contained in a field because it is not an integral domain.

4. Let \( F \) be a field of characteristic \( p \). We proved in class that \( F \) contains the finite field \( \mathbb{Z}/p\mathbb{Z} \) as a subring. Suppose \( a \in F \) satisfies \( a^p = a \). Prove that \( a \) is in the subfield \( \mathbb{Z}/p\mathbb{Z} \).

   Consider the polynomial \( f(x) = x^p - x \in F[x] \). The elements of \( \mathbb{Z}/p\mathbb{Z} \) are zeros of this polynomial, by Fermat’s little theorem. Thus \( f(x) \) has \( p \) distinct zeros, all in \( \mathbb{Z}/p\mathbb{Z} \). Because \( f \) has degree \( p \), those are all of its zeros in the field \( F \). Because \( a^p = a \) in \( F \), \( f(a) = 0 \), so \( a \in \mathbb{Z}/p\mathbb{Z} \).

5. Set \( R = \mathbb{Z}/10\mathbb{Z} \). Give an example of an ideal of \( R \) that is prime. Be sure to prove that your ideal is prime. Is your ideal also maximal?

   Consider the principal ideal \( \langle 2 \rangle \) in \( \mathbb{Z}/10\mathbb{Z} \). By the third isomorphism theorem, \( \mathbb{Z}/10\mathbb{Z}/\langle 2 \rangle = \mathbb{Z}/2\mathbb{Z} \), because \( 2|10 \). This is an integral domain (in fact, a field), so \( \langle 2 \rangle \) is prime.

   We also could have chosen \( \langle 5 \rangle \) as a prime ideal. Recall that prime ideals are by definition proper ideals, so \( \langle 5 \rangle \) and \( \langle 2 \rangle \) are the only options.

6. Are there any examples of ideals of the ring \( R = \mathbb{Z}[i] \) that are prime but not maximal?

   The zero ideal \( \{ 0 \} \) is an example. (In fact, this is the only such example; it is a very good exercise to try to prove that all other prime ideals are maximal!)
7. Suppose $R$ is a commutative ring with unity, and $I \subseteq R$ is a prime ideal so that $R/I$ has finite size. Prove that $I$ is maximal. Give an example of a commutative ring $R$ with unity and an ideal $I$ so that

- $R$ has infinite size and
- $R/I$ has finite size but $I$ is not maximal.

**Proof.** The quotient $R/I$ is a finite integral domain. As such, it is necessarily a field (we proved this!) and therefore $I$ is maximal.

For an example for the second part, we could take $R = \mathbb{Z}$ and $I = (10)$.

8. Let $R = \mathbb{Z}[i]$. Find a prime number $p$ so that $R/\langle p \rangle$ is not an integral domain. Be sure to prove your answer.

**Proof.** By the third isomorphism theorem, $R/\langle p \rangle \cong \mathbb{Z}/p\mathbb{Z}[x]/(x^2 + 1)$. This will fail to be an integral domain as soon as $x^2 + 1$ is reducible over $\mathbb{Z}/p\mathbb{Z}$. One could choose $p = 2$ (then $x^2 + 1 = (x + 1)^2$), $p = 5$ (then $x^2 + 1 = (x + 2)(x - 2)$), $p = 13$ (then $x^2 + 1 = (x + 5)(x - 5)$) or in fact any prime that is equivalent to 1 modulo 4.

9. For each of the following polynomials, factor it into a product of irreducibles. If the polynomial itself is irreducible, then say so. (Be sure to prove your answers.)

(a) $x^2 + 5x + 3 \in \mathbb{Z}/2\mathbb{Z}[x]$.
(b) $x^3 + x^2 + x + 1 \in \mathbb{Q}[x]$. **Hint:** Observe that $-1$ is a root of this polynomial.
(c) $x^4 + 27x^2 + 6 \in \mathbb{Q}[x]$.
(d) $x^3 - x + 1 \in \mathbb{Z}/7\mathbb{Z}[x]$.
(e) $x^3 + 2x + 1 \in \mathbb{Q}[x]$. **Hint:** Consider the same polynomial in $\mathbb{Z}/3\mathbb{Z}[x]$.

**Proof.** We have:

(a) The polynomial $x^2 + 5x + 3$ is irreducible over $\mathbb{Z}/2\mathbb{Z}$, because neither 0 nor 1 are roots.
(b) Because $-1$ is a root, $x + 1$ must be a factor. Using long division gives $x^3 + x^2 + x + 1 = (x + 1)(x^2 + 1)$. The polynomial $x^2 + 1$ is irreducible over $\mathbb{Q}$ as it has no roots in $\mathbb{Q}$ and is quadratic.
(c) The polynomial $x^4 + 27x^2 + 6$ is irreducible over $\mathbb{Q}$ by Eisenstein’s criterion using the prime $p = 3$.
(d) By plugging in different values for $x$, one finds $x = 2$ is a root. Now one does division to factor out an $x - 2$ and obtain $x^3 - x + 1 = (x - 2)(x^2 + 2x + 3)$. By trying the various values modulo 7, one finds $x^2 + 2x + 3$ has no root in $\mathbb{Z}/7\mathbb{Z}$ and thus is irreducible over $\mathbb{Z}/7\mathbb{Z}$.
(e) The polynomial $x^3 + 2x + 1$ is irreducible over $\mathbb{Z}/3\mathbb{Z}$, as one finds by checking that it has no root. Therefore $x^3 + 2x + 1$ is irreducible over $\mathbb{Q}$.
10. Construct explicitly a field of size 49.

Proof. The polynomial $x^2 + 1$ has no root over $\mathbb{Z}/7\mathbb{Z}$, thus is irreducible over this field. Consequently $\mathbb{Z}/7\mathbb{Z}[x]/\langle x^2 + 1 \rangle$ is a field of size $7^2 = 49$. □

11. Is $\mathbb{Z}[\sqrt{5}]/\langle 1 + \sqrt{5} \rangle$ a field? How many elements are in this quotient?

Proof. By the third isomorphism theorem, $\mathbb{Z}[\sqrt{5}]/\langle 1 + \sqrt{5} \rangle \simeq \mathbb{Z}[x]/\langle x^2 - 5, 1 + x \rangle$. Now $x^2 - 5 = (x + 1)(x - 1) - 4$, so $\mathbb{Z}[\sqrt{5}]/\langle 1 + \sqrt{5} \rangle \simeq \mathbb{Z}[x]/\langle x + 1, 4 \rangle$.

Now $\mathbb{Z}[x]/\langle x + 1 \rangle \simeq \mathbb{Z}$ by the map $f(x) \mapsto f(-1)$, so $\mathbb{Z}[x]/\langle x + 1, 4 \rangle \simeq \mathbb{Z}/4\mathbb{Z}$. This is not a field, and has four elements. □

12. Let $R$ be the ring $R = \mathbb{Z}[x]/\langle x^3 + 4x + 1 \rangle$ and let $\alpha$ denote the image of $x$ in $R$. What is the size of the ring $R/\langle \alpha - 1 \rangle$?

Proof. By the third isomorphism theorem, we have $R/\langle \alpha - 1 \rangle \simeq \mathbb{Z}[x]/\langle x - 1, x^3 + 4x + 1 \rangle$.

Now, $x^3 + 4x + 1 = q(x)(x - 1) + 6$, where I quickly found the remainder by plugging in 1 for $x$ in $x^3 + 4x + 1$. Thus $\langle x - 1, x^3 + 4x + 1 \rangle = \langle 6, x - 1 \rangle$, and similar to the previous problem $R/\langle \alpha - 1 \rangle \simeq \mathbb{Z}/6\mathbb{Z}$. Thus this quotient has 6 elements. □

13. Give an example of a ring $R$ that

- Contains the complex numbers $\mathbb{C}$ as a subring;
- As a $\mathbb{C}$ vector space, is of dimension four.

Proof. As a class of examples, we could take $\mathbb{C}[x]/\left\langle f(x) \right\rangle$ where $f(x) \in \mathbb{C}[x]$ is any polynomial of degree four. So, to be concrete, $\mathbb{C}[x]/\langle x^4 \rangle$ would work. □

14. Prove that the rings $\mathbb{Z}[x]/\langle x^2 \rangle$ and $\mathbb{Z} \times \mathbb{Z}$ are not isomorphic.

Proof. Note that in the second ring $\mathbb{Z} \times \mathbb{Z}$, if $\alpha^2 = 0$ then $\alpha = 0$. However, in the first ring, there is the nonzero element $x + \langle x^2 \rangle$ which satisfies $(x + \langle x^2 \rangle)^2 = 0$. □

15. Consider the ring homomorphism $\phi : \mathbb{Q}[x] \to \mathbb{Q}\sqrt{2}$ defined by $\phi(x) = 1 + \sqrt{2}$. Find a polynomial $p(x)$ so that $\ker(\phi) = \langle p(x) \rangle$.

Proof. Because $\phi(x) = 1 + \sqrt{2}$, $\phi(x - 1) = \sqrt{2}$, and thus $\phi((x - 1)^2 - 2) = 0$. We claim that $p(x) = (x - 1)^2 - 2 = x^2 - 2x - 1$ works. Note that we have shown that $\ker(\phi) \supseteq \langle p(x) \rangle$. To see the reverse inclusion, first note that $\phi$ is injective when restricted to polynomials of the form $a + bx$, as $\phi(a + bx) = a + b + b\sqrt{2}$. Now, suppose $g(x) \in \ker(\phi)$. Then we can write $g(x) = q(x)p(x) + a + bx$ for some $a, b \in \mathbb{Q}$. Consequently, $\phi(g(x)) = \phi(a + bx) = 0$ if and only if $a = b = 0$, proving that $g(x) \in \langle p(x) \rangle$. □