Name: _____

Reading Questions

Read Section 5.3, pages 206-211. **You may omit Example 5.15(v) and Example 5.16.** There are only two definitions and one proven result in this part of the reading, but there are a lot of good examples. Read them carefully, making sure to look up references, and work out the details for yourself!

1. What are the two terms that are defined? (Write them here.) Write their definitions, word for word, in your notebook.

2. Reread Example 5.14 and 5.15.

   (a) One of the examples ends with a question. State and answer the question here.

   (b) Are any of the examples unclear? Which ones? Take the time to reread them, look up references, and check the details in your notebook.

   (c) Challenge: Can you think of any additional examples?

3. This section contains a result stating properties of homomorphisms. Write this result, word for word, in your notebook.

4. Example 5.18 states two claims about finite commutative rings, and explains why both claims are true. What are the two claims? Briefly summarize the arguments explaining why the claims are true.

Skim Section 5.3, pages 213-216. The main idea is that when we have a homomorphism of rings $R \to S$, (i) we can extend the homomorphism to a homomorphism $R[x] \to S$ (Theorem 5.19) and (ii) to a homomorphism $R[x] \to S[x]$ (Corollary 5.22). These results have very useful applications.

5. Corollary 5.21 is a useful application of Theorem 5.19. Write the definition of the evaluation homomorphism (given at the top of page 215) and Corollary 5.21 in your notebook, word for word.

   What is $e_3(2 - 3x + x^2)$?

6. Examples 5.23 and 5.24 are useful applications of Corollary 5.22.

   (a) If $r_2 : \mathbb{Z} \to \mathbb{Z}_2$ is reduction modulo 2, what is $r_2^*(3 + 2x + 5x^2)$?

   (b) If $c : \mathbb{C} \to \mathbb{C}$ is complex conjugation, what is $c^*((2 + 4i) + (2 + 3i)x + x^2)$?

7. What struck you in this reading? What is still unclear? What remaining questions do you have?

Name: _____

Read Section 5.3, pages 216-220, Kernel, Image, and Ideals.

Reading Questions

1. Write the definitions of the kernel and image of a homomorphism in your notebook, word for word, and study the examples given in Example 5.26. If any of these examples are unclear to you, take the time to reread them and work out the details in your notebook.

2. Write the definition of an ideal in your notebook, word for word. Restate Proposition 5.25 as two claims (instead of three) using the word ideal.

3. The author points out that we have seen ideals in this class outside the context of kernels. In particular, one of the exercises from Section 1.3, on page 30, can be reformulated in terms of ideals in $\mathbb{Z}$. What problem is it? Restate this problem using the word ideal.

4. List (here) the additional terminology defined on page 218 and 219. Take notes in your notebook.

5. Simple examples of ideals are given in Example 5.27. Make sure you understand these. Pay particular attention to 5.27(iv).

6. Example 5.30 contains a result worth remembering. Summarize the example here. (The power of this result is illustrated in Corollary 5.32.)

7. Write Proposition 5.31 in your notebook, word for word, and look at the proof. Take the time to fill in the details of the proof for yourself, if there are any parts that are unclear to you.

8. What struck you in this reading? What is still unclear? What remaining questions do you have?

Name: _____

Read Section 6.1, pages 233-242, up to and including Proposition 6.4.

Reading Questions

1. On pages 233-234, there are three terms that are defined for a general commutative ring. State the terms here, and write their definitions in your notebook, word for word.

2. Lemma 6.1 is very useful and is used in the proofs of many of the other propositions in this section. Read through the proof again, making sure to look up any references. Would this proposition be true if k were merely a domain and not necessarily a field?

3. Proposition 6.2 describes the units in $k[x]$, where k is a field. This result is also used in the proofs of many results in this section. Reread the proof. Compare with Exercise 5.14.

   Would the proof still work if k were merely a domain and not necessarily a field?

4. Reread Proposition 6.4 and its proof. Find a monic associate for $4x^2 + 6x + 11$ in $\mathbb{Q}[x]$. Does $4x^2 + 6x + 11$ have a monic associate in $\mathbb{Z}[x]$? Explain.

5. What struck you in this reading? What is still unclear? What remaining questions do you have?

Name: _____

Read Section 6.1, pages 234-242. **You may omit Example 6.7 and Proposition 6.21.**

Reading Questions

1. With the exception of Proposition 6.6(i), all the results in this part of the section are about polynomial rings. Most of the results are about $k[x]$, where k is a field. The two main results are analogues of Proposition 1.14 and Theorem 1.15, namely Proposition 6.8 and Theorem 6.11. Write both of these results in your notebook, word for word, and briefly summarize them here.

2. Proposition 6.5 gives a useful criterion for irreducibility in $k[x]$, where k is a field. Remember that the results about $k[x]$ in this section are analogues of results about $\mathbb{Z}$. Reread Proposition 6.5, and try to formulate the analogous statement for $\mathbb{Z}$.

   Hint: Nonzero constants in $k[x]$ are the units in $k[x]$. So saying that f is a nonconstant polynomial means that f is not the zero polynomial and f is not a unit in $k[x]$. The analogue in $\mathbb{Z}$ is an integer m that is nonzero and not a unit (i.e. $m \neq \pm 1$). Irreducibles in $\mathbb{Z}$ are $\pm p$ for primes p. The analogue of degree in $k[x]$ is absolute value in $\mathbb{Z}$.

3. What do you think the analogue of Proposition 6.6(ii) would be for $\mathbb{Z}$? (Hint: The analogue of a monic polynomial is a positive integer.)

4. Proposition 6.13 will be useful for future discussions about roots of unity. List all the polynomials of the form $x^m - 1$, for $0 < m \in \mathbb{Z}$, that are divisors of $x^{12} - 1$.

5. The first four results in the part about roots build on each other: the Remainder Theorem is used to prove the Factor Theorem, the Factor Theorem is used to prove Theorem 6.16, and Theorem 6.16 is used to prove Proposition 6.18. Take some notes on them. The Factor Theorem and Theorem 6.16 are generally useful; write these in your notebook word for word.

6. Give an example to show that Theorem 6.16 is not true for polynomials with coefficients in an arbitrary commutative ring.

7. Study the proof of Proposition 6.18. Would this proof work if k was a finite field? Prove or give a counterexample.

8. What struck you in this reading? What is still unclear? What remaining questions do you have?

Name: _____

Read Section 6.1, pages 243-251, on GCDs, Euclid's Lemma, and the Euclidean Algorithm.

Reading Questions

1. Write the definition of a gcd of two polynomials in $k[x]$ (where k is a field) in your notebook, word for word. Why do we define a gcd to be monic?

2. Theorem 6.25 is the analogue of Theorem 5.29. The outline of the proof should be familiar to you by now! Make sure you understand it. Rereading the proof of Theorem 5.29 may help.

3. Reread Example 5.27(iv) and Corollary 6.26, with its proof. Suppose J is the ideal in $\mathbb{Q}[x]$ consisting of all polynomials having $\sqrt{2}$ as a root. Can you think of a polynomial $d(x) \in \mathbb{Q}[x]$ such that $J = (d)$?

4. Theorem 6.28, Corollary 6.29, Theorem 6.31, Corollary 6.32, and Proposition 6.33 all have analogues in Section 1.3. What are the analogues? (You don't need to give the statement of the results, just the names, e.g. "Theorem 1.X.")

5. Pages 249-251 discuss the Euclidean Algorithm for polynomials in $k[x]$, where k is a field. Recall that the Euclidean Algorithm is basically a repeated use of the Division Algorithm. You may find it helpful to review the Euclidean Algorithm for integers (p 32-33). Read through Examples 6.35, 6.36,

6.39 to see how the Euclidean Algorithm works for polynomials. Notice that the computations quickly become cumbersome, and the authors use a computer to do the long division. (Also, make sure to see the correction to Example 6.39.)

In Example 6.39, the gcd of $f(x) = x^3 - 2x^2 + x - 2$ and $g(x) = x^4 - 1$ is computed. What is it? What are the coefficients s and t such that $\gcd(f, g) = s\,f + t\,g$? (Make sure to see the correction to Example 6.39.)

6. What struck you in this reading? What is still unclear? What remaining questions do you have?

Name: _____

Read Section 6.1, pages 252-258, on unique factorization, PIDs, and UFDs.

Reading Questions

1. Write Theorem 6.40 word for word in your notebook. The exact wording is important. Theorem 6.40, Proposition 6.41, and Corollary 6.42 all have analogues in Section 2.1. What are the analogues? (You don't need to give the statement of the results, just the names, e.g. "Theorem 2.X.")

2. The last paragraph before the exercises defines the *multiplicity* of a root. Construct an example for yourself to make this definition more concrete. (Pick your favorite number r to be a root and your favorite positive integer e to be the multiplicity of the root. Construct a polynomial that has r as a root with multiplicity e.)

3. Write the definition of a PID in your notebook, word for word, and study Example 6.44, especially (i)-(iv), making sure to look up references. For (iii), you might want to look back at Example 5.30(ii).

4. By definition, every PID is a domain. Is every domain a PID? Is every field a PID? Is every PID a field? Support your claims with references to examples or proven results.

5. Write the definition of a gcd in a PID in your notebook, word for word. Does this match the definition given for a gcd in $\mathbb{Z}$ or $k[x]$?

6. In the next several pages, the author generalizes the discussion of unique factorization in $\mathbb{Z}$, given in Section 2.1, and unique factorization in $k[x]$, given in the preceding parts of Section 6.1, to prove unique factorization in an abstract PID.

7. Write the definition of a UFD in your notebook, word for word.

8. Reread the paragraphs after the definition of UFD. By definition, every UFD is a domain. Is every domain a UFD? Is every PID a UFD? Is every UFD a PID? Support your claims with references to examples or proven results.

9. What struck you in this reading? What is still unclear? What remaining questions do you have?

Name: _____

Read the first part of Section 6.2, Irreducibility, pages 259-263.

Reading Questions

1. This section contains several irreducibility criteria (i.e. results of the form "If ..., then $f(x)$ is irreducible in (*some polynomial ring.*)" Write them, word for word, in your notebook.

2. One of these criteria (Proposition 6.51) is useful only for polynomials of low degree. Use this criterion, along with the Rational Root Theorem (Theorem 6.52), to show that $x^2 + x + 1$ is irreducible in $\mathbb{Q}[x]$.

3. The Rational Root Theorem is useful because it allows us to reduce the list of possible roots from an infinite list (every rational number) to a finite list (rational numbers of a certain form.) This is also the reason why reduction modulo p (for prime p) is useful. Recall that $\mathbb{F}_p$ is the (unique!) finite field with p elements. Thus $\mathbb{F}_p$ is the same as $\mathbb{Z}_p$. (See page 205.)

   Show that $x^2 + x + 1$ is irreducible in $\mathbb{F}_2[x]$ by checking all the possible roots (namely [0] and [1]) and applying Proposition 6.51.

   What does this allow us to conclude about $x^2 + x + 1$ as a polynomial in $\mathbb{Q}[x]$? (See Proposition/Theorem 6.55.)

4. Reread Examples 6.56 and 6.57.

   (a) List all the monic quadratic polynomials in $\mathbb{F}_3[x]$.

   (b) Check for yourself that the only monic irreducible quadratics in $\mathbb{F}_3[x]$ are x^2+1, x^2+x-1, and x^2-x-1.

5. What struck you in this reading? What is still unclear? What remaining questions do you have?

Name: _____

Read the supplemental notes on complex powers and roots (along with the relevant parts of Section 3.3, as needed) and finish reading Section 6.2, Roots of Unity, pages 264-268.

Reading Questions

1. This part of Section 6.2 contains one irreducibility criterion. What is it's name? Write it, word for word, in your notebook.

2. Write the definition of the d^{th} cyclotomic polynomial in your notebook, along with Proposition 6.60.

   (a) Use the table on page 266 (note the corrections!) to verify Proposition 6.60 for $n = 6$, i.e. using the formulas for $\Phi_1(x)$, $\Phi_2(x)$, $\Phi_3(x)$, $\Phi_6(x)$ given in the table, verify directly that $x^6 - 1 = \Phi_1(x)\,\Phi_2(x)\,\Phi_3(x)\,\Phi_6(x)$.

   (b) Use the table on page 266 (note the corrections!) to write the factorization of $x^{12} - 1$ into irreducible factors.

3. What struck you in this reading? What is still unclear? What remaining questions do you have?

Name: _____

Read the introduction to Chapter 7 and Section 7.1, Quotient Rings, pages 277-284.

This section generalizes the construction of the commutative ring, $\mathbb{Z}_m$, from the ring of integers, $\mathbb{Z}$. As the authors develop the theory for a general ring, R and ideal I, they tell you where to find the corresponding results for $\mathbb{Z}_m$. Be sure to look back at those results when directed to do so. Familiarity with $\mathbb{Z}$ and $\mathbb{Z}_m$ will help you in understanding the generalization.

Reading Questions

1. For any ideal I in a commutative ring R, "congruence mod I" can be used to build another commutative ring that generalizes the construction of $\mathbb{Z}_m$ from $\mathbb{Z}$. Describe the construction of this quotient ring, R/I, in your notebook.

   Describe the elements of R/I (what are these elements called?) and the addition and multiplication in R/I.

   What is the zero of this ring?

   What is the multiplicative identity in this ring?

2. For the ideal $I = (x^2 - 2)$ in $\mathbb{Z}[x]$, compute the product $(x + 3 + I)(x^2 + 2x - 1 + I)$ in the quotient ring $\mathbb{Z}[x]/I$. Hint: Since "$x^2 - 2 = 0$" in $\mathbb{Z}[x]/I$, "$x^2 = 2$" in $\mathbb{Z}[x]/I$.

3. In Proposition 7.8, we define the natural map $\pi : R \to R/I$ by $a \to a + I$, and prove that this is a surjective homomorphism. Write the definition of this homomorphism in your notebook. What precisely is this map in the case where $R = \mathbb{Z}$ and $I = (m)$?

4. Write the statement of Theorem 7.10, the First Isomorphism Theorem, in your notebook, word for word. What conclusion does this theorem allow you to make about the commutative ring $\mathbb{Z}_m$? Does this makes sense to you?

5. Theorem 7.11 tells us that if $I = (x^2 + 1)$, then $\mathbb{R}[x]/I$ is a field isomorphic to $\mathbb{C}$. Compute the product $(2x + 3 + I)(3x - 4 + I)$ in $\mathbb{R}[x]/(x^2 + 1)$.

   Find the inverse of $(2x + 3 + I)$ in $\mathbb{R}[x]/(x^2 + 1)$ (i.e. find a, $b \in \mathbb{R}$, such that $(2x + 3 + I)(ax + b + I) = 1 + I$.)

6. What struck you in this reading? What is still unclear? What remaining questions do you have?