MAT 411: Introduction to Abstract Algebra
Final Exam (Take-Home Portion)

Your Name:

Names of Any Collaborators:

Instructions

This portion of the Final Exam is worth a total of 16 points and is due by **5pm on Thursday, December 14**. Your total combined score on the in-class portion and take-home portion is worth 18% of your overall grade.

I expect your solutions to be *well-written, neat, and organized.* Do not turn in rough drafts. What you turn in should be the "polished" version of potentially several drafts.

Feel free to type up your final version. The LaTeX source file of this exam is also available if you are interested in typing up your solutions using LaTeX. I'll gladly help you do this if you'd like.

The simple rules for the exam are:

1. You may freely use any theorems that we have discussed in class, but you should make it clear where you are using a previous result and which result you are using. For example, if a sentence in your proof follows from Theorem 1.41, then you should say so.
2. Unless you prove them, you cannot use any results from the course notes that we have not yet covered.
3. You are **NOT** allowed to consult external sources when working on the exam. This includes people outside of the class, other textbooks, and online resources.
4. You are **NOT** allowed to copy someone else's work.
5. You are **NOT** allowed to let someone else copy your work.
6. You are allowed to discuss the problems with each other and critique each other's work.

I will vigorously pursue anyone suspected of breaking these rules.

You should **turn in this cover page** and all of the work that you have decided to submit. **Please write your solutions and proofs on your own paper.**

To convince me that you have read and understand the instructions, sign in the box below.

Signature:

Good luck and have fun!

Introduction

The discussion that follows is a summary of Sections 10.3 and 10.4 of the course notes. You'll need these ideas for some of the problems that follow (but not all of the problems). If you've already looked over Sections 10.3 and 10.4, then you can just skip to the problems.

Recall that if G is a group and H is a subgroup of G, then we can form the quotient group G/H exactly when H is normal in G. We would like to mimic the same construction for rings. That is, if R is a ring and I is a subring, we would like to form the quotient ring R/I. Since R is an abelian group under addition, all subrings will automatically be normal subgroups under addition. That is, if we ignore multiplication R/I is a well-defined group under addition of cosets. In this case, the cosets are of the form $r + I$, where $r \in R$. If $r + I$ and $s + I$ are two (additive) cosets of I, then we add just like we did for groups:

$$(r + I) + (s + I) = (r + s) + I.$$

But if we want to make a ring out of R/I, we need to be able to multiply cosets. The natural choice is:

$$(r + I)(s + I) = (rs) + I.$$

Analogous to the situation for groups (where we could only quotient by a normal subgroup), multiplication of cosets is only well-defined under certain circumstances. The following definition is exactly the condition on the subring that we need in order for multiplication of cosets to be well-defined. You can think of this definition as the analog of "normal" for rings.

Definition 10.40. Let R be a ring and let I be a subring of R.

(a) I is a **left ideal** (respectively, **right ideal**) of R if $rI \subseteq I$ (respectively, $Ir \subseteq I$) for all $r \in R$.

(b) I is an **ideal** (or **two-sided ideal**) if I is both a left and a right ideal.

Recall that a subring must be closed under multiplication. An ideal is a special kind of subring with the property that we can multiply elements of the ideal by whatever we want and we never leave the subring. There is a rather lengthy discussion in Section 10.3 that argues that we can form a quotient ring exactly when we quotient by an ideal. That is, we have the following theorem (which is proved in the course notes).

Theorem 10.41. Let R be a ring and let I be an ideal of R. Then the additive quotient group R/I is a ring under the binary operations:

$$(r + I) + (s + I) = (r + s) + I$$
$$(r + I)(s + I) = (rs) + I$$

for all $r, s \in R$. Conversely, if I is any subgroup such that the above operations are well-defined, then I is an ideal of R.

Here are a few quick observations that I'll let you ponder. Assume R is a ring and let I be an ideal of R.

(a) The additive identity in R/I is $0 + I$.

(b) If R is a commutative ring, then R/I is also a commutative ring.

(c) If R is a ring with 1, say 1_R, then R/I is also a ring with 1. In this case, the multiplicative identity is $1_R + I$.

(d) If $r \in R$ is a unit (i.e., r^{-1} exists), then $(r + I)$ is a unit, namely $(r + I)^{-1} = r^{-1} + I$. However, it's possible that $r + I$ is a unit even if r is not.

Definition 10.45. Assume that R is a ring with multiplicative identity $1 \neq 0$. For any subset A of R, let (A) denote the smallest ideal of R containing A, called the **ideal generated by** A. If A consists of a single element, say $A = \{a\}$, then $(a) := (\{a\})$ is called a **principal ideal**.

Loosely speaking, you should think of principal ideals as being analogous to cyclic subgroups. Note that if R is commutative, then

$$(a) = aR := \{ar \mid r \in R\}.$$

As you might expect, we have an isomorphism theorem for rings. The proof of the following theorem is more or less identical to the proof of the First Isomorphism Theorem for groups.

Theorem 10.43. (First Isomorphism Theorem for Rings) If $\phi : R \to S$ is a ring homomorphism, then $\ker(\phi)$ is an ideal of R and $R/\ker(\phi) \cong \phi(R)$.

A couple of the problems below require the following definition.

Definition 10.52. Assume R is a commutative ring with 1. An ideal M in a ring R is called a **maximal ideal** if $M \neq R$ and the only ideals containing M are M and R.

See Example 10.53 in the course notes for a few examples involving maximal ideals.

Problems

(4 points each) Complete **four** of the following problems. You are allowed to use the results of an earlier problem in the proof of a later problem (even if you did not complete the earlier problem). However, you may not use a later result in the proof of an earlier problem. For example, you can use the results of Problem 5 to complete Problem 7, but not the other way around.

1. Prove that any finite integral domain is a field.

   Note: This is Theorem 10.25 in the course notes.

   Hint: Let R be a finite integral domain. Then among other things, R has a 1, say 1_R. Let $a \in R \setminus \{0\}$. Define $\phi_a : R \to R$ via $\phi_a(r) = ar$. Verify that ϕ_a is a ring homomorphism such that $\ker(\phi_a) = \{0\}$. Then by Theorem 9.12, ϕ_a is one-to-one. Is ϕ_a onto? If so, then there exists r in domain of function that maps to 1_R.

2. Let $\phi : R \to S$ be a ring homomorphism. Prove that $\ker(\phi)$ is an ideal of R.

   Note: This verifies the first claim in the First Isomorphism Theorem for Rings given above.

   Hint: Your proof must also argue that $\ker(\phi)$ is a subring (see Remark 10.29). We already know that $\ker(\phi)$ is a subgroup under addition, so use this fact to shorten your proof. It's enough to check that $\ker(\phi)$ is a left ideal. Notice that proving that $\ker(\phi)$ is closed under multiplication by any ring element from R will prove that $\ker(\phi)$ is closed under multiplication.

3. Consider the ideal $(2, x)$ in $\mathbb{Z}[x]$. Note that $(2, x) = \{2p(x) + xq(x) \mid p(x), q(x) \in \mathbb{Z}[x]\}$. Prove that $(2, x)$ is not a principal ideal, i.e., there is no single polynomial in $\mathbb{Z}[x]$ that we can use to generate $(2, x)$.

   Note: This is Problem 10.48 in the course notes.

4. Assume R is a commutative ring with $1 \neq 0$. Let I be an ideal of R. Prove that if I contains a unit, then $I = R$.

   Note: This is half of Theorem 10.49 in the course notes. The converse is also true, which you may use in later problems if you wish.

5. Assume R is a commutative ring with $1 \neq 0$. Prove that if the only ideals of R are $\{0\}$ and R, then R is a field.

   Note: This is half of Theorem 10.50 in the course notes. The converse is also true.

6. Prove that if R is a field, then every nonzero ring homomorphism from R into another ring is one-to-one.

   Note: This is Corollary 10.51 in the course notes.

7. Assume R is a commutative ring with 1. Prove that if M is maximal ideal, then R/M is a field.

   Note: This is half of Theorem 10.55 in the course notes. The converse is also true.

   Hint: Try using a proof by contradiction. Assume that R/M is not a field. Then by the contrapositive Problem 5, there exists an ideal J/M of R/M, where J is a subring of R such that $M \subset J \subset R$ $(J \neq M, R)$. Now, let $r \in R$ and $j \in J$. Compute $(r + J)(j + J)$ and using the fact that J/M is an ideal, prove that J is an ideal, which contradicts M being maximal.

8. Consider the polynomial ring $\mathbb{Z}[x]$ (see Example 10.26(g)) and let

$$I = \{p(x) \in \mathbb{Z}[x] \mid p(x) \text{ has constant term equal to } 0\}.$$

   Note that I is an ideal (you do not need to prove this) and happens to be the smallest ideal containing the polynomial $f(x) = x$. Use Problem 7 together with the First Isomorphism Theorem for Rings to prove that I is not a maximal ideal of $\mathbb{Z}[x]$.

