189-235A: Algebra I
Assignment 4
Due: Monday, November 12

1. Let R be a commutative ring. Is the set S of matrices of the form $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$, with $a, b, c \in R$, a subring of $M_2(R)$?

2. Show that the ring $\mathbf{Q}$ of rational numbers has no subrings which are finite sets.

3. Let $R = \mathbf{Q}(\sqrt{2})$ be the ring of elements of the form $a + b\sqrt{2}$, with $a, b \in \mathbf{Q}$. Show that the function which sends $a + b\sqrt{2}$ to $a - b\sqrt{2}$ is an isomorphism from R to itself.

4. Let R be a ring. Show that there is a *unique* ring homomorphism f from $\mathbf{Z}$ to R.

5. Show that a ring R which is a finite set and an integral domain (has no zero-divisors) is necessarily a field.

Which of the following subsets I of a commutative ring R are ideals of R? Justify your answer.

6. $R = F[X]$, where F is a field, and $I = F$ is the set of constant polynomials.

7. $R = \mathbf{Z} \times \mathbf{Z}$, and $I = \{(m, 0) \quad \text{where } m \in \mathbf{Z}\}$.

8. The set of *nilpotent elements* of a commutative ring R, i.e., those $a \in R$ such that $a^n = 0$ for some n. What if R is not commutative?

9. R is the ring of functions from $\mathbf{Z}$ to the real numbers $\mathbf{R}$, and I the subset of those functions f satisfying $f(0) = f(1)$.

10. R is the ring of functions from $\mathbf{Z}$ to $\mathbf{R}$, and I the subset of those functions f satisfying $f(0) = f(1) = 0$.

11. Let R be the polynomial ring $F[x]$ with coefficients in a field. Show that every ideal of R is principal. Give an example of an ideal in $\mathbf{Z}[x]$ which is not principal.

12. Show that the quotient ring $\mathbf{R}[x]/(x^2 + 1)$ is isomorphic to $\mathbf{C}$, and that $\mathbf{C}[x]/(x^2 + 1)$ is isomorphic to $\mathbf{C} \times \mathbf{C}$.

The following exercises are optional. They are not much more difficult than the other exercises, but you will need some extra time to work them out. If you do you will be rewarded with a glimpse of some of the important questions, and ensuing results, which led to the birth of ring theory in its modern form.

Let $\mathbf{Q}(\sqrt{-5}) = \{a + b\sqrt{-5}, a, b \in \mathbf{Q}\}$, and $\mathbf{Z}[\sqrt{-5}] = \{a + b\sqrt{-5}, a, b \in \mathbf{Z}\}$.

13. Show that $\mathbf{Q}(\sqrt{-5})$ is a field, and that $\mathbf{Z}[\sqrt{-5}]$ is a subring. It is called the *ring of integers* of $\mathbf{Q}(\sqrt{-5})$ and plays the role of the usual integers in the arithmetic of $\mathbf{Q}(\sqrt{-5})$.

14. Show that the invertible elements in $\mathbf{Z}[\sqrt{-5}]$ are exactly 1 and -1.

15. Show that the elements 2, 3, $1+\sqrt{-5}$ and $1-\sqrt{-5}$ are irreducible. (I.e., they cannot be written in the form ab where $a, b \neq \pm 1$.)

16. Using 15, show that the ring $\mathbf{Z}[\sqrt{-5}]$ is not a unique factorization ring. (I.e., the "integers" in $\mathbf{Z}[\sqrt{-5}]$ cannot be written uniquely as a product of irreducible elements.)

17. Show that the ideals $(2, 1+\sqrt{-5})$, $(3, 1+\sqrt{-5})$, and $(3, 1-\sqrt{-5})$ are not principal, and that they are *irreducible*, i.e.,they cannot be factored further into products of non-trivial ideals.

18. If I and J are ideals, define the product IJ to be the ideal generated by

the elements of the form ij with $i \in I$ and $j \in J$. Show that $(2, 1+\sqrt{5})^2 = (2)$, $(3, 1+\sqrt{-5})(3, 1-\sqrt{-5}) = (3)$, and conclude that the ideal (6) factorizes as a product of 4 (non-principal) ideals:

$$(6) = (2, 1+\sqrt{-5})^2(3, 1+\sqrt{-5})(3, 1-\sqrt{-5}).$$

Remark: It can be shown that this factorization of the principal ideal (6) into a product of irreducible ideals is *unique*, up to the order of the factors. This is a general phenomenon: although the ring $\mathbf{Z}[\sqrt{-5}]$ fails to satisfy unique factorization, its *ideals* can be expressed uniquely as products of irreducible ideals. The introduction of ideals in the late 19-*th* century by Dedekind was an attempt to salvage unique factorization in such rings, by showing it was true on the level of ideals which were viewed as a kind of "ideal number". This is where the terminology comes from...