Modern Algebra, Review for Final Exam

As with the first two one-hour exams, the final exam be divided into three sections: a section on definitions and statements of important results, a section on examples and calculations, and a section on proofs of elementary results. The final exam will be worth **150 points** (as opposed to 200 points). The length of the final will be roughly proportional. For example, in the "Proofs" section, you will be given a number of problems, from which you will be asked to choose **5**. Of these, you will be responsible for doing at least **2** proofs involving ring theory.

Roughly 50% of the Final Exam will consist of material from the first two examinations; the remaining 50% will be taken from the material on *ring theory*. This review will be composed solely of ring theory material; in order to prepare for the earlier material (*group theory* and *set theory*), you are advised to refer to the earlier two reviews and exams.

I. Definitions, Concepts and Statements of Important Results.

Note: Please remember that we require all of our rings to have a multiplicative identity, usually denoted "1." Not all authors make such as assumption.

1. Let $(R, +, \cdot)$ be a ring and let $S \subseteq R$. What does it mean to say that S is a *subring* of R? [*Remember:* there's a simple criterion for S to be a subring of R, *viz.,* that S be closed under addition and multiplication, and that $1 \in S$.]
2. If R is a ring and $0 \neq a \in R$, what does it mean to say that a is a *zero-divisor*?
3. If R is a commutative ring, what does it mean to say that R is an *integral domain*?
4. If R is a ring, and $u \in R$, what does it mean to say that u is a *unit* in R. [*Note:* in the text, Herstein calls the multiplicative identity the *unit* (see *page* 126). However, this is a bit nonstandard; it's much more commonplace to call any element having a multiplicative inverse a unit.]
5. If R is a commutative ring, what does it mean to say that R is a *field*?
6. If R, R' are rings and if $\phi : R \to R'$ is a mapping, what does it mean to say that ϕ is a *homomorphism* from R to R'?
7. If $\phi : R \to R'$ is a homomorphism of rings, define $\ker \phi$, the *kernel* of the homomorphism ϕ.
8. Is the kernel of a ring homomorphism $\phi : R \to R'$ a subring of R?

9. If R is a ring and if $I \subseteq R$ is a subset, what does it mean to say that I is an *ideal* of R?
10. If R is a commutative ring and if $I \subseteq R$ is an ideal, what does it mean to say that I is a *principal ideal* of R?
11. If R is a ring and if $I, J \subseteq R$ are ideals, how does one define the *sum* $I + J$ of the ideals of I, J?
12. Is the kernel of a ring homomorphism $\phi : R \to R'$ necessarily an ideal of R?
13. If R is a ring, and if $I \subseteq R$ is an ideal, how does one define R/I, the *quotient ring* of R, *modulo* I? What issues of well-definedness arise?
14. Suppose that $\phi : R \to R'$ is a surjective ring homomorphism. What does the *Fundamental Homomorphism Theorem* say in this context?
15. If R is a ring and if $P \subseteq R$ is an ideal, what does it mean to say that P is a *prime ideal* of R?
16. How does the ideal $P \subseteq R$ being prime relate to the structure of the quotient ring R/P?
17. If R is a ring and if $M \subseteq R$ is an ideal, what does it mean to say that M is a *maximal ideal* of R?
18. How does the ideal $M \subseteq R$ being maximal relate to the structure of the quotient ring R/M?
19. Let $\mathbf{F}$ be a field and let $\mathbf{F}[x]$ be the ring of polynomials with coefficients in the field $\mathbf{F}$. What does the *division algorithm* say for $\mathbf{F}[x]$?
20. If R is any commutative ring, and if $p \in R$, what does it mean to say that

    p is an *irreducible* element of R?

    p is a *prime*?
21. Are irreducible polynomials always prime?
22. In general, are irreducible elements always prime?
23. If R is a commutative ring, and if p is a prime element, must p be irreducible?
24. Let $\mathbf{F}$ be a field and let $\alpha \in \mathbf{F}$. How does one define the *evaluation homomorphism* $E_\alpha : \mathbf{F}[x] \to \mathbf{F}$?
25. If $\mathbf{F}$ is a field and if $f(x) \in \mathbf{F}[x]$, what does it mean for the element $\alpha \in \mathbf{F}$ to be a *root* of $f(x)$?
26. How does the divisibility of $f(x)$ by $x - \alpha$ relate to whether or not α is a root of $f(x)$?

27. What does the *Fundamental Theorem of Arithmetic* say for the ring $\mathbf{F}[x]$ of polynomials?

II. Examples and Calculations.

1. Give an example of a zero divisor in the rings
   (a) $\mathbf{Z}/(12)$;
   (b) The matrix ring
$$R = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbf{Q} \right\}.$$
2. Find all the zero divisors in the ring $\mathbf{Z}/(12)$.
3. In the ring $\mathbf{Z}[\sqrt{-5}]$ give an example of an irreducible element that is not prime.
4. In each case below, construct a ring homomorphism $R \to R'$:
   (a) $R = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \mid a, b, c \in \mathbf{Q} \right\}$, $R' = \mathbf{Q}$;
   (b) $R = \mathbf{Z}[i]$ (*Gaussian integers*), $R' = \mathbf{Z}/(5)$;
   (c) $R = \mathbf{Z}[\sqrt{2}]$, $R' = \mathbf{Z}/(7)$;
   (d) $R = \mathbf{Q}[x]$, $R' = \mathbf{Q}$.
5. In each case below, give an example of an ideal $I \subseteq R$ $(I \neq \{0\}, I \neq R)$:
   (a) $R = \mathbf{Z}$;
   (b) $R = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \mid a, b, c \in \mathbf{Z} \right\}$;
   (c) $R = \mathbf{Z}[i]$;
   (d) $R = \mathbf{F}[x]$, where $\mathbf{F}$ is a field.
6. Let $R = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \mid a, b, c \in \mathbf{Z} \right\}$, and define $\phi : R \to \mathbf{Z}/(2)$ by setting
$$\phi\left(\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \right) = [a]_2.$$
   Compute $\ker \phi$.
7. In each case below, give an example of a prime ideal $P \supseteq I$, where $I \subseteq R$ are given below:
   (a) $I = (6) \subseteq \mathbf{Z}$;
   (b) $I = (x^3 + x^2 + x + 1) \subseteq \mathbf{Q}[x]$.

   Are the examples you gave also *maximal* ideals?

8. Suppose that $f(x) = x^{99} - 5x^{49} + 1 \in \mathbf{Q}[x]$. Compute the remainder when $f(x)$ is divided by
   (a) x;
   (b) $x - 1$;
   (c) $x + 1$.
9. Give an example of an irreducible polynomial $f(x) \in \mathbf{F}[x]$ having degree at least 2 where $\mathbf{F}$ is as below:
   (a) $\mathbf{R}$;
   (b) $\mathbf{Q}$;
   (c) $\mathbf{Z}/(2)$;
   (d) $\mathbf{Z}/(3)$:
10. Let $\mathbf{F} = \mathbf{Z}/(2)$ and factor the polynomial $x^8 + x \in \mathbf{F}[x]$ into irreducible factors.
11. Let $f(x) = x^2 + x + 1$. Is $f(x)$ irreducible when regarded as an element of
    (a) $\mathbf{R}[x]$;
    (b) $\mathbf{Q}[x]$;
    (c) $\mathbf{Z}/(2)[x]$;
    (d) $\mathbf{Z}/(3)[x]$;
    (e) $\mathbf{Z}/(5)[x]$.
12. If $\mathbf{F}$ is the field $\mathbf{F} = \mathbf{Z}/(3)$, it is easy to check that the polynomial $x^2 + 1 \in \mathbf{F}[x]$ is irreducible; as a result it follows that $\mathbf{K} = \mathbf{F}/(x^2 + 1)$ is a field. If we set $\alpha = x + (x^2 + 1) \in \mathbf{K}$, compute $(\alpha - 1)^3$ in terms of the elements $0, 1, 2, \alpha, 1 + \alpha, 2 + \alpha, 2\alpha, 1 + 2\alpha, 2 + 2\alpha$.

III. Proofs.

1. Let R be an integral domain and assume that $ab = ac$, where $a, b, c \in R$ and $a \neq 0$. Prove that $b = c$.
2. In each case below, you are given a mapping $\phi : R \to R'$.
   (a) Let $R = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \mid a, b, c \in \mathbf{Q} \right\}$, $R' = \mathbf{Q}$, and define $\phi : R \to R'$ by setting
   $$\phi\left(\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \right) = a - c.$$
   Is ϕ a ring homomorphism? Prove your assertion.

(b) Again, let $R = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \mid a, b, c \in \mathbf{Q} \right\}$, $R' = \mathbf{Q}$, and define

$$\phi\left(\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}\right) = a.$$

Prove that ϕ is a ring homomorphism.

(c) Here, $R = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \mid a, b, c \in \mathbf{Z} \right\}$, $R' = \mathbf{Z}/(n)$, where n is a positive integer. Set

$$\phi\left(\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}\right) = [c]_n,$$

and show that ϕ is a homomorphism of rings.

(d) $R = \mathbf{Z}[i]$, $R' = \mathbf{Z}/(5)$ and $\phi(a + bi) = [a - 2b]_5 \in \mathbf{Z}/(5)$. Show that ϕ is a ring homomorphism.

(e) $R = \mathbf{Z}[\sqrt{2}]$, $R' = \mathbf{Z}/(7)$, $\phi(a + b\sqrt{2}) = [a + 3b]_7 \in \mathbf{Z}/(7)$. Show that ϕ is a ring homomorphism.

3. Let R, R' be rings, and let $\phi : R \to R'$ be a mapping such that $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2), \phi(r_1 \cdot r_2) = \phi(r_1) \cdot \phi(r_2)$. If R' is an integral domain, show that ϕ is a ring homomorphism. [The only thing missing, of course, is that $\phi(1) = 1'$, where $1, 1'$ are the multiplicative identities of R, R', respectively.]

4. Prove that the ring $\mathbf{Z}/(n)$ is an integral domain if and only if n is prime.

5. Let R be a commutative ring and let $I \subseteq R$ be an ideal. Prove that I is a prime ideal if and only if R/I is an integral domain.

6. Let R be a commutative ring and let $I \subseteq R$ be an ideal. Prove that I is a maximal ideal if and only if R/I is a field.

7. Let R be a commutative ring. Prove that R is a field if and only if the only ideals of R are $\{0\}$ and R itself.

8. Let m, n be relatively prime integers and define the mapping $\mathbf{Z} \xrightarrow{\phi} \mathbf{Z}/(m) \times \mathbf{Z}/(n)$ by setting $\phi(a) = ([a]_m, [a]_n) \in \mathbf{Z}/(m) \times \mathbf{Z}/(n)$.

(a) Show that ϕ is a ring homomorphism.

(b) Compute $\ker \phi$.

(c) Show that ϕ is onto. [This is a bit more difficult, unless you look at this in exactly the right way.]

9. Let

$$R = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbf{Q} \right\},$$

and define $I \subseteq R$ by setting

$$I = \left\{ \begin{bmatrix} a & 0 \\ c & 0 \end{bmatrix} \mid a, c \in \mathbf{Q} \right\}.$$

Show that I is a left ideal of R.

10. Let $f(x), g(x)$ be relatively prime polynomials in $\mathbf{F}[x]$ and assume that $f(x)|h(x)$, $g(x)|h(x)$. Prove that $f(x)g(x)|h(x)$.