HW 1

7.1

7. The *center* of a ring R is $\{z \in R \mid zr = rz \text{ for all } r \in R\}$ (i.e., is the set of all elements which commute with every element of R). Prove that the center of a ring is a subring that contains the identity. Prove that the center of a division ring is a field.

15. A ring R is called a *Boolean ring* if $a^2 = a$ for all $a \in R$. Prove that every Boolean ring is commutative.

21. Let X be any nonempty set and let $\mathcal{P}(X)$ be the set of all subsets of X (the *power set* of X). Define addition and multiplication on $\mathcal{P}(X)$ by

$$A + B = (A - B) \cup (B - A) \qquad \text{and} \qquad A \times B = A \cap B$$

i.e., addition is symmetric difference and multiplication is intersection.

(a) Prove that $\mathcal{P}(X)$ is a ring under these operations ($\mathcal{P}(X)$ and its subrings are often referred to as *rings of sets*).

(b) Prove that this ring is commutative, has an identity and is a Boolean ring.

26. Let K be a field. A *discrete valuation* on K is a function $\nu : K^\times \to \mathbb{Z}$ satisfying

(i) $\nu(ab) = \nu(a) + \nu(b)$ (i.e., ν is a homomorphism from the multiplicative group of nonzero elements of K to $\mathbb{Z}$),

(ii) ν is surjective, and

(iii) $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$ for all $x, y \in K^\times$ with $x + y \neq 0$.

The set $R = \{x \in K^\times \mid \nu(x) \geq 0\} \cup \{0\}$ is called the *valuation ring* of ν.

(a) Prove that R is a subring of K which contains the identity. (In general, a ring R is called a *discrete valuation ring* if there is some field K and some discrete valuation ν on K such that R is the valuation ring of ν.)

(b) Prove that for each nonzero element $x \in K$ either x or x^{-1} is in R.

(c) Prove that an element x is a unit of R if and only if $\nu(x) = 0$.

27. A specific example of a discrete valuation ring (cf. the preceding exercise) is obtained when p is a prime, $K = \mathbb{Q}$ and

$$\nu_p : \mathbb{Q}^\times \to \mathbb{Z} \qquad \text{by} \qquad \nu_p\left(\frac{a}{b}\right) = \alpha \quad \text{where } \frac{a}{b} = p^\alpha \frac{c}{d}, \quad p \nmid c \text{ and } p \nmid d.$$

Prove that the corresponding valuation ring R is the ring of all rational numbers whose denominators are relatively prime to p. Describe the units of this valuation ring.

7.2

5. Let F be a field and define the ring $F((x))$ of *formal Laurent series* with coefficients from F by

$$F((x)) = \{\sum_{n \geq N}^{\infty} a_n x^n \mid a_n \in F \text{ and } N \in \mathbb{Z}\}.$$

(Every element of $F((x))$ is a power series in x plus a polynomial in $1/x$, i.e., each element of $F((x))$ has only a finite number of terms with negative powers of x.)

(a) Prove that $F((x))$ is a field.

(b) Define the map

$$\nu : F((x))^{\times} \to \mathbb{Z} \qquad \text{by} \qquad \nu(\sum_{n \geq N}^{\infty} a_n x^n) = N$$

where a_N is the first nonzero coefficient of the series (i.e., N is the "order of zero or pole of the series at 0"). Prove that ν is a discrete valuation on $F((x))$ whose discrete valuation ring is $F[[x]]$, the ring of formal power series (cf. Exercise 26, Section 1).

6. Let S be a ring with identity $1 \neq 0$. Let $n \in \mathbb{Z}^+$ and let A be an $n \times n$ matrix with entries from S whose i, j entry is a_{ij}. Let E_{ij} be the element of $M_n(S)$ whose i, j entry is 1 and whose other entries are all 0.

(a) Prove that $E_{ij}A$ is the matrix whose i^{th} row equals the j^{th} row of A and all other rows are zero.

(b) Prove that AE_{ij} is the matrix whose j^{th} column equals the i^{th} column of A and all other columns are zero.

(c) Deduce that $E_{pq}AE_{rs}$ is the matrix whose p, s entry is a_{qr} and all other entries are zero.

7. Prove that the center of the ring $M_n(R)$ is the set of scalar matrices (cf. Exercise 7, Section 1). [Use the preceding exercise.]

7.3

13. Prove that the ring $M_2(\mathbb{R})$ contains a subring that is isomorphic to $\mathbb{C}$.

14. Prove that the ring $M_4(\mathbb{R})$ contains a subring that is isomorphic to the real Hamilton Quaternions, $\mathbb{H}$.

26. The *characteristic* of a ring R is the smallest positive integer n such that $1+1+\cdots+1=0$ (n times) in R; if no such integer exists the characteristic of R is said to be 0. For example, $\mathbb{Z}/n\mathbb{Z}$ is a ring of characteristic n for each positive integer n and $\mathbb{Z}$ is a ring of characteristic 0.

(a) Prove that the map $\mathbb{Z} \to R$ defined by

$$k \mapsto \begin{cases} 1+1+\cdots+1 \ (k \text{ times}) & \text{if } k > 0 \\ 0 & \text{if } k = 0 \\ -1-1-\cdots-1 \ (-k \text{ times}) & \text{if } k < 0 \end{cases}$$

is a ring homomorphism whose kernel is $n\mathbb{Z}$, where n is the characteristic of R (this explains the use of the terminology "characteristic 0" instead of the archaic phrase "characteristic ∞" for rings in which no sum of 1's is zero).

(b) Determine the characteristics of the rings $\mathbb{Q}$, $\mathbb{Z}[x]$, $\mathbb{Z}/n\mathbb{Z}[x]$.

(c) Prove that if p is a prime and if R is a commutative ring of characteristic p, then $(a+b)^p = a^p + b^p$ for all $a, b \in R$.

7.4

2. Assume R is commutative. Prove that the augmentation ideal in the group ring RG is generated by $\{g-1 \mid g \in G\}$. Prove that if $G = \langle \sigma \rangle$ is cyclic then the augmentation ideal is generated by $\sigma - 1$.

3. (a) Let p be a prime and let G be an abelian group of order p^n. Prove that the nilradical of the group ring $\mathbb{F}_pG$ is the augmentation ideal (cf. Exercise 29, Section 3). [Use the preceding exercise.]

(b) Let $G = \{g_1, \dots, g_n\}$ be a finite group and assume R is commutative. Prove that if r is any element of the augmentation ideal of RG then $r(g_1 + \cdots + g_n) = 0$. [Use the preceding exercise.]

13. Let $\varphi : R \to S$ be a homomorphism of commutative rings.

(a) Prove that if P is a prime ideal of S then either $\varphi^{-1}(P) = R$ or $\varphi^{-1}(P)$ is a prime ideal of R. Apply this to the special case when R is a subring of S and φ is the inclusion homomorphism to deduce that if P is a prime ideal of S then $P \cap R$ is either R or a prime ideal of R.

(b) Prove that if M is a maximal ideal of S and φ is surjective then $\varphi^{-1}(M)$ is a maximal ideal of R. Give an example to show that this need not be the case if φ is not surjective.

14. Assume R is commutative. Let x be an indeterminate, let $f(x)$ be a monic polynomial in $R[x]$ of degree $n \geq 1$ and use the bar notation to denote passage to the quotient ring $R[x]/(f(x))$.

(a) Show that every element of $R[x]/(f(x))$ is of the form $\overline{p(x)}$ for some polynomial $p(x) \in R[x]$ of degree less than n, i.e.,

$$R[x]/(f(x)) = \{\overline{a_0} + \overline{a_1 x} + \cdots + \overline{a_{n-1}x^{n-1}} \mid a_0, a_1, \ldots, a_{n-1} \in R\}.$$

[If $f(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_0$ then $\overline{x^n} = \overline{-(b_{n-1}x^{n-1} + \cdots + b_0)}$. Use this to reduce powers of $\overline{x}$ in the quotient ring.]

(b) Prove that if $p(x)$ and $q(x)$ are distinct polynomials in $R[x]$ which are both of degree less than n, then $\overline{p(x)} \neq \overline{q(x)}$. [Otherwise $p(x) - q(x)$ is an $R[x]$-multiple of the monic polynomial $f(x)$.]

(c) If $f(x) = a(x)b(x)$ where both $a(x)$ and $b(x)$ have degree less than n, prove that $\overline{a(x)}$ is a zero divisor in $R[x]/(f(x))$.

(d) If $f(x) = x^n - a$ for some nilpotent element $a \in R$, prove that $\overline{x}$ is nilpotent in $R[x]/(f(x))$.

(e) Let p be a prime, assume $R = \mathbb{F}_p$ and $f(x) = x^p - a$ for some $a \in \mathbb{F}_p$. Prove that $\overline{x-a}$ is nilpotent in $R[x]/(f(x))$. [Use Exercise 26(c) of Section 3.]

19. Let R be a finite commutative ring with identity. Prove that every prime ideal of R is a maximal ideal.

40. Assume R is commutative. Prove that the following are equivalent: (see also Exercises 13 and 14 in Section 1)

(i) R has exactly one prime ideal

(ii) every element of R is either nilpotent or a unit

(iii) $R/\eta(R)$ is a field (cf. Exercise 29, Section 3).

other

Exercise A. Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be ideals in a commutative ring R, and let $\mathfrak{p}$ be a prime ideal of R with $\mathfrak{p} \supset \bigcap_{i=1}^n \mathfrak{a}_i$. Show that $\mathfrak{p} \supset \mathfrak{a}_i$ for some i.

Exercise B. Prove the following properties of the radical of an ideal:

(a) $\mathrm{rad}(\mathfrak{a}) \supset \mathfrak{a}$.
(b) $\mathrm{rad}(\mathrm{rad}(\mathfrak{a})) = \mathrm{rad}(\mathfrak{a})$.
(c) $\mathrm{rad}(\mathfrak{a}\mathfrak{b}) = \mathrm{rad}(\mathfrak{a} \cap \mathfrak{b}) = \mathrm{rad}(\mathfrak{a}) \cap \mathrm{rad}(\mathfrak{b})$.
(d) $\mathrm{rad}(\mathfrak{a}) = (1)$ if and only if $\mathfrak{a} = (1)$.
(e) $\mathrm{rad}(\mathfrak{a} + \mathfrak{b}) = \mathrm{rad}(\mathrm{rad}(\mathfrak{a}) + \mathrm{rad}(\mathfrak{b}))$.
(f) If $\mathfrak{p}$ is prime, then $\mathrm{rad}(\mathfrak{p}^n) = \mathfrak{p}$ for all $n > 0$.

Conclude that if $R = \mathbb{Z}$ and $\mathfrak{a} = (m)$ for $m \in \mathbb{Z}_{>1}$ with prime factorization $m = \prod_{i=1}^{t} p_i^{r_i}$, then
$$\mathrm{rad}(m) = (p_1 \cdots p_t).$$

HW2

7.5

3. Let R and S be rings with identities. Prove that every ideal of $R \times S$ is of the form $I \times J$ where I is an ideal of R and J is an ideal of S.

4. Prove that if R and S are nonzero rings then $R \times S$ is never a field.

5. Let $n_1, n_2, \ldots, n_k$ be integers which are relatively prime in pairs: $(n_i, n_j) = 1$ for all $i \neq j$.
   (a) Show that the Chinese Remainder Theorem implies that for any $a_1, \ldots, a_k \in \mathbb{Z}$ there is a solution $x \in \mathbb{Z}$ to the simultaneous congruences
$$x \equiv a_1 \bmod n_1, \qquad x \equiv a_2 \bmod n_2, \qquad \ldots, \qquad x \equiv a_k \bmod n_k$$
   and that the solution x is unique mod $n = n_1 n_2 \ldots n_k$.
   (b) Let $n_i' = n/n_i$ be the quotient of n by n_i, which is relatively prime to n_i by assumption. Let t_i be the inverse of n_i' mod n_i. Prove that the solution x in (a) is given by
$$x = a_1 t_1 n_1' + a_2 t_2 n_2' + \cdots + a_k t_k n_k' \bmod n.$$
   Note that the elements t_i can be quickly found by the Euclidean Algorithm as described in Section 2 of the Preliminaries chapter (writing $an_i + bn_i' = (n_i, n_i') = 1$ gives $t_i = b$) and that these then quickly give the solutions to the system of congruences above for any choice of $a_1, a_2, \ldots, a_k$.
   (c) Solve the simultaneous system of congruences
$$x \equiv 1 \bmod 8, \qquad x \equiv 2 \bmod 25, \qquad \text{and} \qquad x \equiv 3 \bmod 81$$
   and the simultaneous system
$$y \equiv 5 \bmod 8, \qquad y \equiv 12 \bmod 25, \qquad \text{and} \qquad y \equiv 47 \bmod 81.$$

15.4

21. Suppose $\varphi : R \to S$ is a ring homomorphism and D' is a multiplicatively closed subset of S. Let $D = \varphi^{-1}(D')$. Prove that D is a multiplicatively closed subset of R and that the map $\varphi' : D^{-1}R \to D'^{-1}S$ given by $\varphi'(r/d) = \varphi(r)/\varphi(d)$ is a ring homomorphism.

22. Suppose $P \subseteq Q$ are prime ideals in R and let R_Q be the localization of R at Q. Prove that the localization R_P is isomorphic to the localization of R_Q at the prime ideal PR_Q (cf. the preceding exercise).

23. Let $\varphi : A \to B$ be a homomorphism of commutative rings with $\varphi(1_A) = 1_B$, and let P be a prime ideal of A. Let contraction and extension of ideals with respect to φ be denoted by superscripts c and e respectively. Prove that P is the contraction of a prime ideal in B if and only if $P = (P^e)^c$. [Localize B at $\varphi(A - P)$.]

other

Exercise A. Let R, R' be commutative rings, let $S \subset R$ be a multiplicative subset, and let $f : R \to S^{-1}R$ be the natural map $r \mapsto \frac{r}{1}$.

Show that if $g : R \to R'$ is a ring homomorphism satisfying the following three properties:

(1) for all $s \in R$, $g(s)$ is a unit in R',
(2) if $g(r) = 0$, then $rs = 0$ for some $s \in S$,
(3) every element of R' is of the form $g(r)g(s)^{-1}$ for some $r \in R$ and $s \in S$,

then there exists a unique ring isomorphism $h : S^{-1}R \xrightarrow{\sim} R'$ such that $g = h \circ f$.

Exercise B. Let R be a commutative ring, $\mathfrak{p} \subset R$ a prime ideal, and $S = R \setminus \mathfrak{p}$ (a multiplicative subset of R). Then we know that the localization $R_\mathfrak{p} := S^{-1}R$ is a local ring with unique maximal ideal $\mathfrak{p}R_\mathfrak{p} := S^{-1}\mathfrak{p}$.

Show that there is an isomorphism

$$\mathrm{Frac}(R/\mathfrak{p}) \xrightarrow{\sim} R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$$

between the field of fractions of the integral domain $R/\mathfrak{p}$ and the residue field of the local ring $R_\mathfrak{p}$.

10.1

5. For any left ideal I of R define

$$IM = \{\sum_{\text{finite}} a_i m_i \mid a_i \in I,\ m_i \in M\}$$

to be the collection of all finite sums of elements of the form am where $a \in I$ and $m \in M$. Prove that IM is a submodule of M.

8. An element m of the R-module M is called a *torsion element* if $rm = 0$ for some nonzero element $r \in R$. The set of torsion elements is denoted

$$\mathrm{Tor}(M) = \{m \in M \mid rm = 0 \text{ for some nonzero } r \in R\}.$$

(a) Prove that if R is an integral domain then $\mathrm{Tor}(M)$ is a submodule of M (called the *torsion* submodule of M).

(b) Give an example of a ring R and an R-module M such that $\mathrm{Tor}(M)$ is not a submodule. [Consider the torsion elements in the R-module R.]

(c) If R has zero divisors show that every nonzero R-module has nonzero torsion elements.

15. If M is a finite abelian group then M is naturally a $\mathbb{Z}$-module. Can this action be extended to make M into a $\mathbb{Q}$-module?

18. Let $F = \mathbb{R}$, let $V = \mathbb{R}^2$ and let T be the linear transformation from V to V which is rotation clockwise about the origin by $\pi/2$ radians. Show that V and 0 are the only $F[x]$-submodules for this T.

10.2

4. Let A be any $\mathbb{Z}$-module, let a be any element of A and let n be a positive integer. Prove that the map $\varphi_a : \mathbb{Z}/n\mathbb{Z} \to A$ given by $\varphi(\bar{k}) = ka$ is a well defined $\mathbb{Z}$-module homomorphism if and only if $na = 0$. Prove that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A) \cong A_n$, where $A_n = \{a \in A \mid na = 0\}$ (so A_n is the annihilator in A of the ideal (n) of $\mathbb{Z}$ — cf. Exercise 10, Section 1).

6. Prove that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/(n, m)\mathbb{Z}$.

9. Let R be a commutative ring. Prove that $\mathrm{Hom}_R(R, M)$ and M are isomorphic as left R-modules. [Show that each element of $\mathrm{Hom}_R(R, M)$ is determined by its value on the identity of R.]

12. Let I be a left ideal of R and let n be a positive integer. Prove

$$R^n/IR^n \cong R/IR \times \cdots \times R/IR \quad (n \text{ times})$$

where IR^n is defined as in Exercise 5 of Section 1. [Use the preceding exercise.]

13. Let I be a nilpotent ideal in a commutative ring R (cf. Exercise 37, Section 7.3), let M and N be R-modules and let $\varphi : M \to N$ be an R-module homomorphism. Show that if the induced map $\overline{\varphi} : M/IM \to N/IN$ is surjective, then φ is surjective.

10.3

2. Assume R is commutative. Prove that $R^n \cong R^m$ if and only if $n = m$, i.e., two free R-modules of finite rank are isomorphic if and only if they have the same rank. [Apply Exercise 12 of Section 2 with I a maximal ideal of R. You may assume that if F is a field, then $F^n \cong F^m$ if and only if $n = m$, i.e., two finite dimensional vector spaces over F are isomorphic if and only if they have the same dimension — this will be proved later in Section 11.1.]

4. An R-module M is called a *torsion* module if for each $m \in M$ there is a nonzero element $r \in R$ such that $rm = 0$, where r may depend on m (i.e., $M = \operatorname{Tor}(M)$ in the notation of Exercise 8 of Section 1). Prove that every finite abelian group is a torsion $\mathbb{Z}$-module. Give an example of an infinite abelian group that is a torsion $\mathbb{Z}$-module.

7. Let N be a submodule of M. Prove that if both M/N and N are finitely generated then so is M.

12. Let R be a commutative ring and let A, B and M be R-modules. Prove the following isomorphisms of R-modules:

(a) $\operatorname{Hom}_R(A \times B, M) \cong \operatorname{Hom}_R(A, M) \times \operatorname{Hom}_R(B, M)$

(b) $\operatorname{Hom}_R(M, A \times B) \cong \operatorname{Hom}_R(M, A) \times \operatorname{Hom}_R(M, B)$.

HW3

10.5

2. Suppose that

$$\begin{tikzcd} A \arrow[r] \arrow[d, "\alpha"'] & B \arrow[r] \arrow[d, "\beta"'] & C \arrow[r] \arrow[d, "\gamma"'] & D \arrow[d, "\delta"'] \\ A' \arrow[r] & B' \arrow[r] & C' \arrow[r] & D' \end{tikzcd}$$

is a commutative diagram of groups, and that the rows are exact. Prove that

(a) if α is surjective, and β, δ are injective, then γ is injective.

(b) if δ is injective, and α, γ are surjective, then β is surjective.

3. Let P_1 and P_2 be R-modules. Prove that $P_1 \oplus P_2$ is a projective R-module if and only if both P_1 and P_2 are projective.

4. Let Q_1 and Q_2 be R-modules. Prove that $Q_1 \oplus Q_2$ is an injective R-module if and only if both Q_1 and Q_2 are injective.

7. Let A be a nonzero finite abelian group.

(a) Prove that A is not a projective $\mathbb{Z}$-module.

(b) Prove that A is not an injective $\mathbb{Z}$-module.

27. Let M, A and B be R-modules.

(a) Suppose $f : A \to M$ and $g : B \to M$ are R-module homomorphisms. Prove that $X = \{(a, b) \mid a \in A,\ b \in B \text{ with } f(a) = g(b)\}$ is an R-submodule of the direct sum $A \oplus B$ (called the *pullback* or *fiber product* of f and g) and that there is a commutative diagram

$$\begin{tikzcd} X \arrow[r, "\pi_2"] \arrow[d, "\pi_1"'] & B \arrow[d, "g"'] \\ A \arrow[r, "f"] & M \end{tikzcd}$$

where π_1 and π_2 are the natural projections onto the first and second components.

(b) Suppose $f' : M \to A$ and $g' : M \to B$ are R-module homomorphisms. Prove that the quotient Y of $A \oplus B$ by $\{(f'(m), -g'(m)) \mid m \in M\}$ is an R-module (called the *pushout* or *fiber sum* of f' and g') and that there is a commutative diagram

$$\begin{tikzcd} M \arrow[r, "g'"] \arrow[d, "f'"'] & B \arrow[d, "\pi_2'"] \\ A \arrow[r, "\pi_1'"] & Y \end{tikzcd}$$

where π_1' and π_2' are the natural maps to the quotient induced by the maps into the first and second components.

28. **(a)** *(Schanuel's Lemma)* If $0 \to K \to P \xrightarrow{\varphi} M \to 0$ and $0 \to K' \to P' \xrightarrow{\varphi'} M \to 0$ are exact sequences of R-modules where P and P' are projective, prove $P \oplus K' \cong P' \oplus K$ as R-modules. [Show that there is an exact sequence $0 \to \ker \pi \to X \xrightarrow{\pi} P \to 0$ with $\ker \pi \cong K'$, where X is the fiber product of φ and φ' as in the previous exercise. Deduce that $X \cong P \oplus K'$. Show similarly that $X \cong P' \oplus K$.]

(b) If $0 \to M \to Q \xrightarrow{\psi} L \to 0$ and $0 \to M \to Q' \xrightarrow{\psi'} L' \to 0$ are exact sequences of R-modules where Q and Q' are injective, prove $Q \oplus L' \cong Q' \oplus L$ as R-modules.

The R-modules M and N are said to be *projectively equivalent* if $M \oplus P \cong N \oplus P'$ for some projective modules P, P'. Similarly, M and N are *injectively equivalent* if $M \oplus Q \cong N \oplus Q'$ for some injective modules Q, Q'. The previous exercise shows K and K' are projectively equivalent and L and L' are injectively equivalent.