Section 7.1

11. Prove that if R is an integral domain and $x^2 = 1$ for some $x \in R$ then $x = \pm 1$.

Proof. (Buchholz) Let $x \in R$ where $x^2 = 1$. Then

$$\begin{aligned} x^2 &= 1 \\ x^2 - 1 &= 0 \\ (x-1)(x+1) &= 0 \end{aligned}$$

So $(x-1) = 0$ or $(x+1) = 0$, but R was an integral domain which implies that R has no zero divisors. Therefore $x = 1$ or $x = -1$. □

13. *An element x in R is called* **nilpotent** *if $x^m = 0$ for some $m \in \mathbb{Z}^+$.*

(a) Show that if $n = a^k b$ for some integers a and b then $\overline{ab}$ is a nilpotent element of $\mathbb{Z}/n\mathbb{Z}$

Proof. Let $n = a^k b$ for some $a, b \in \mathbb{Z}$ then

$$(ab)^k = (a^k b)b^{k-1} = nb^{k-1}$$

hence $(ab)^k \equiv 0 \mod n$. □

(b) If $a \in \mathbb{Z}$ is integer, show that the element $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ is a nilpotent if and only if every prime divisor of n is also a divisor of a. In particular determine the nilpotent elements of $\mathbb{Z}/72\mathbb{Z}$ explicitly.

Proof. ($\Rightarrow$) Let $a \in \mathbb{Z}$ and $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ is a nilpotent, and let p be a prime divisor of n (i.e. $p|n$). Since $a^k \equiv 0 \mod n$, then $p|a^k$, hence $p|a$, since p is a prime number.

($\Leftarrow$) Suppose $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$, then $a = p_1^{\gamma_1} p_2^{\gamma_2} ... p_k^{\gamma_k}$ with $1 \leq \gamma_i \leq \alpha_i$ for each prime p_i. Let m be the maximum of the α_i. Then $n \,\big|\, a^m$ and thus, $a^m \equiv 0 \mod n$. It follows that $\bar{a}$ is a nilpotent element of $\mathbb{Z}/n\mathbb{Z}$. □

The nilpotent elements of $\mathbb{Z}/72\mathbb{Z}$ are $0, 6, 12, 18, 24, 30, 36, 42, 48, 54, 60, 66$.

(c) Let R be a ring of functions from nonempty set X to a field F. Prove that R contains no nonzero nilpotent element

Proof. Let f be a nonzero nilpotent element in R then there exist $x \in X$ s.t. $f(x) \neq 0$. Since f is nilpotent, then $f^k \equiv 0$ for some $k \in \mathbb{Z}^+$, then $f^k(x) = [f(x)]^k = 0$ from which it follows that $f(x) = 0$, but this is a contradiction. Hence R contains no nonzero nilpotent element. □

14. *Let x be a nilpotent of the commutative ring R*

(a) Prove that x is either zero or zero divisor.

Proof. If $x = 0$ then we are done.

Let $x \neq 0$ and let k be minimal element in $\mathbb{Z}^+$ s.t. $x^k = 0$, since x is a nilpotent, then $xx^{k-1} = 0$ where $x^{k-1} \neq 0$. Therefore x is a zero divisor. □

(b) Prove that rx is nilpotent for all $r \in R$.

Proof. $(rx)^k = r^k x^k = r^k 0 = 0$ hence rx is nilpotent for all $r \in R$. □

(c) Prove that $1+x$ is a unit in R.

Proof.
$$(1+x)(1-x+x^2-x^3+...+(-1)^{m-1}x^{m-1})=1$$
□

(d) Deduce that the sum of nilpotent element and a unit is a unit.

Proof. Let $u+x$ be the sum of nilpotent element x and a unit u. Then $u+x=u(1+u^{-1}x)$, from part (a) $u^{-1}x$ is a nilpotent, by part (b) $1+u^{-1}x$ is a unit, so multiplication of two unit elements of R is equal to a unit element in R. □

18. The set $S=\{(r,r)|r\in R\}$ is a subring of $R\times R$.

Proof. (Gillispie) By definition $S\subset R\times R$.
Pick $a,b\in R$. So $(a,a)+(-b,-b)=(a-b,a-b)\in S$ and so $(S,+)\leq(R,+)$.
S inherits the associative and distributive laws from $R\times R$.
Finally $(a,a)\cdot(b,b)=(ab,ab)\in R$ and so R is closed under multiplication and S is a subring of R. □

Chapter 7.2

2. Follow hint in book.

3. Define the set $R[[x]]$ of formal power series in the indeterminate x with coefficients from R to be all formal infinite
$$\sum_{n=0}^{\infty}a_nx^n=a_0+a_1x+a_2x^2+a_3x^3+\dots.$$
Define addition and multiplication of power series in the same way as for power series with real or complex coefficients i.e., extend polynomial addition and multiplication to power series as though they were "polynomials of infinite degree":
$$\sum_{n=0}^{\infty}a_nx^n+\sum_{n=0}^{\infty}b_nx^n=\sum_{n=0}^{\infty}(a_n+b_n)x^n$$
$$\sum_{n=0}^{\infty}a_nx^n\times\sum_{n=0}^{\infty}b_nx^n=\sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}a_kb_{n-k}\right)x^n.$$

   a. Prove that $R[[x]]$ is a commutative ring with 1.

   Proof. (Hazlett) Note, a technical proof that $+$ and $\times$ are associative can be written. We will exclude these. Let $p,q\in R[[x]]$ where
   $$p=\sum_{n=0}^{\infty}a_nx^n, q=\sum_{n=0}^{\infty}b_nx^n.$$
   Then
   $$p+q=\sum_{n=0}^{\infty}a_nx^n+\sum_{n=0}^{\infty}b_nx^n=\sum_{n=0}^{\infty}(a_n+b_n)x^n.$$
   Each $a_n+b_n\in R$ so $p+q\in R[[x]]$. Let $0=\sum_{n=0}^{\infty}c_nx^n$ where $c_n=0_R$ for all n. Then
   $$p+0=\sum_{n=0}^{\infty}(a_n+0_R)x^n=\sum_{n=0}^{\infty}a_nx^n=p.$$

Similarly $0 + p = 0$. Set $-p = \sum_{n=0}^{\infty} -a_n x^n$. We know that $-p \in R[[x]]$ since each $-a_n \in R$ because R is a ring. Hence

$$p + (-p) = \sum_{n=0}^{\infty} (a_n - a_n)x^n = \sum_{n=0}^{\infty} 0_R x^n = 0.$$

This implies every element of $R[[x]]$ has an additive inverse. It is clear that since R is an abelian group that $R[[x]]$ is also abelian. Consequently we have $R[[x]]$ is an abelian group under addition. Select $r \in R[[x]]$ where the coefficients of r are c_n. Then

$$\begin{aligned}
p(q + r) &= \sum_{n=0}^{\infty} a_n x^n \times \left(\sum_{n=0}^{\infty} b_n x^n + \sum_{n=0}^{\infty} c_n x^n \right) \\
&= \sum_{n=0}^{\infty} a_n x^n \times \sum_{n=0}^{\infty} (b_n + c_n) x^n \\
&= \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k (b_{n-k} + c_{n-k}) \right) x^n \\
&= \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k b_{n-k} \right) x^n + \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k c_{n-k} \right) x^n \\
&= pq + pr.
\end{aligned}$$

We conclude that multiplication is distributive. We also can see that multiplication is commutative by noting that the coefficient of x^n in pq is $\sum_{k=0}^{n} a_k b_{n-k} = a_0 b_n + a_1 b_{n-1} + a_2 b + n - 2 + \ldots + a_{n-1} b_1 + a_n b_0 = b_0 a_n + b_1 a_{n-1} + \ldots + b_{n-1} a_1 + b_n a_0$, which is the coefficient of x^n in qp. Denote $1 = \sum_{k=0}^{\infty} d_n x^n$ where $d_0 = 1_R$ and $d_n = 0$ for $n > 0$. Then

$$p \cdot 1 = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k d_{n-k} \right) x^n = \sum_{n=0}^{\infty} a_n x^n = p.$$

Since $R[[x]]$ is commutative we have 1 is the multiplicative identity. Therefore $R[[x]]$ is a commutative ring with a 1. □

b. Show that $1 - x$ is a unit in $R[[x]]$ with inverse $1 + x + x^2 + \ldots$.

Proof. (Hazlett) Consider $(1 - x)(1 + x + x^2 + \ldots)$. Note, this is equal to $1(1 + x + x^2 + \ldots) - x(1 + x + x^2 + \ldots) = 1 + x + x^2 + \ldots - x - x^2 - x^3 - \ldots = 1 + (x - x) + (x^2 - x^2) + \ldots = 1$. Therefore $(1 - x)(1 + x + x^2 + \ldots) = 1$ and $(1 - x)$ is a unit with inverse $1 + x + x^2 + \ldots$. □

c. Prove that $\sum_{n=0}^{\infty} a_n x^n$ is a unit in $R[[x]]$ if and only if a_0 is a unit in R.

Proof. (Hazlett) Suppose $\sum_{n=0}^{\infty} a_n x^n$ is a unit. Then there exists some $\sum_{n=0}^{\infty} b_n x^n$ where

$$\sum_{n=0}^{\infty} a_n x^n \times \sum_{n=0}^{\infty} b_n x^n = 1.$$

Note, the constant term of this product is $a_0 b_0 = 1$. Therefore a_0 is a unit with inverse b_0. Assume instead then that a_0 is a unit. Set $a_0^{-1} = c_0$. We want to find a series $\sum_{n=0}^{\infty} c_n x^n$ such that

$$\sum_{n=0}^{\infty} a_n x^n \times \sum_{n=0}^{\infty} c_n x^n = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k c_{n-k} \right) x^n = 1.$$

Specifically we need $a_0 c_0 = 1$, which we have from above, and $\sum_{k=0}^{n} a_k c_{n-k} = 0$ for $n \geq 1$. We will proceed by induction on n. For $n = 1$ we need $a_0 c_1 + a_1 c_0 = 0$. Then $c_1 = -a_0^{-1} a_1 c_0$,

which exists because a_0^{-1} exists. So suppose c_ℓ exists for all ℓ such that $1 \leq \ell < n$. Set $c_n = -a_0^{-1}(a_1c_{n-1} + a_2c_{n-2} + \ldots + a_nc_0)$. Then

$$\begin{aligned}\sum_{k=0}^{n} a_k c_{n-k} &= a_0c_n + a_1c_{n-1} + a_2c_{n-2} + \ldots + a_nc_0 \\ &= -a_0a_0^{-1}(a_1c_{n-1} + a_2c_{n-2} + \ldots + a_nc_0) + a_1c_{n-1} + a_2c_{n-2} + \ldots + a_nc_0 \\ &= 0.\end{aligned}$$

Consequently we can find a series $\sum_{n=0}^{\infty} c_n x^n$ where

$$\sum_{n=0}^{\infty} a_n x^n \times \sum_{n=0}^{\infty} c_n x^n = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k c_{n-k} \right) x^n = 1.$$

Therefore $\sum_{n=0}^{\infty} a_n x^n$ is a unit. □

8. Let S be any ring and let $n \geq 2$ be an integer. Prove that if A is any strictly upper triangular matrix in $M_n(S)$ then $A^n = 0$.

Proof. (Hazlett) We claim that in the matrix $B = (b_{i,j}) = A^\ell$ we have $b_{i,j} = 0$, if $i < j + \ell - 1$. We proceed by induction. The case for $\ell = 1$ is clear from the fact that A is upper triangular. Let $\ell = 2$. Hence, $B = A^2$. Then $b_{i,j} = \sum_{k=1}^{n} a_{i,k}a_{k,j}$. Thus $b_{i,j} = 0$ for $i < k$ and $k < j$. This implies $b_{i,j} = 0$ for $i < j + 1 = j + \ell - 1$. So suppose that $B = A^\ell$ and $b_{i,j} = 0$ for $i < j + \ell - 1$. Set $C = A^{\ell+1}$. Thus $C = AA^\ell = AB$. Then $c_{i,j} = \sum_{k=1}^{n} a_{i,k}b_{k,j}$. Hence $c_{i,j} = 0$ for $i < k$ and $k < j + \ell - 1$. So $c_{i,j} = 0$ for $i < j + \ell = j + (\ell + 1) - 1$, as desired. Let $D = A^n$. Then $d_{i,j} = 0$ for all $i < j + n - 1$. Since D is a $n \times n$ matrix we have $i < j + n - 1$ for all i, j. Therefore $D = 0$. □

9. Let $\alpha = r + r^2 - 2s$ and $\beta = -3r^2 + rs$ be the two elements of the integral group ring $\mathbb{Z}D_8$ described in this section. Compute the following elements of $\mathbb{Z}D_8$:

   a. $\beta\alpha = -3 - 2r - 3r^3 + s + 6r^2s + r^3s$
   b. $\alpha^2 = 5 + r^2 + 2r^3 - 2rs - 4r^2s - 2r^3s$
   c. $\alpha\beta - \beta\alpha = 2r - 2r^3 - s + r^2s$
   d. $\beta\alpha\beta = 15r + 10r^2 + 7r^3 - 21s - 6rs - 5r^2s$

Chapter 7.3

1. Let R be a ring with identity $1 \neq 0$. Prove that the rings $2\mathbb{Z}$ and $3\mathbb{Z}$ are not isomorphic.

Proof. Suppose there is an isomorphism $\varphi : 2\mathbb{Z} \to 3\mathbb{Z}$. Let $\varphi(2) = 3m$, where $m \in \mathbb{Z}^*$ (If $m = 0$, $\varphi(2) = 3 \times 0 = 0$ then $\varphi(2\mathbb{Z}) = \{0\}$, which contradicts our assumption φ is an isomorphism).

Consider $\varphi(4)$, $\varphi(4) = \varphi(2 + 2) = 3m + 3m = 6m$. On the other hand, $\varphi(4) = \varphi(2 \times 2) = 3m \times 3m = 9m^2$. While $m \in \mathbb{Z}^*$, $6m \neq 9m^2$. Thus φ is not an isomorphism, and the rings $2\mathbb{Z}$ and $3\mathbb{Z}$ are not isomorphic. □

4. Find all ring homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}/30\mathbb{Z}$. In each case describe the kernel and the image.

Proof. Let's assume there is a homomorphism φ from $\mathbb{Z}$ to $\mathbb{Z}/30\mathbb{Z}$. Since 1 generates the entire $\mathbb{Z}$ (by addition) let's consider its homomorphic image in $\mathbb{Z}/30\mathbb{Z}$. Let $\varphi(1) = \overline{a}$ for some $\overline{a} \in \mathbb{Z}/30\mathbb{Z}$, then for any $m \in \mathbb{Z}$ we have $\varphi(m) = m \cdot \overline{a} = \overline{am}$. It is easy to check φ preserves the operation of addition. To ensure φ is a ring homomorphism, take any $m, n \in \mathbb{Z}$, we need to satisfy $\varphi(mn) = \varphi(m)\varphi(n)$,

i.e., $\overline{amn} = \overline{am} \times \overline{an} = \overline{a^2mn}$. This forces $\overline{a} = \overline{a^2}$. In $\mathbb{Z}/30\mathbb{Z}$, $\overline{0}, \overline{1}, \overline{6}, \overline{10}, \overline{15}, \overline{16}, \overline{21}, \overline{25}$ satisfies this relationship for $\overline{a}$. Thus the homomorphisms (φ) from $\mathbb{Z}$ to $\mathbb{Z}/30\mathbb{Z}$ are:

Homomorphism	Kernel	Image in $\mathbb{Z}/30\mathbb{Z}$
$\varphi(m) = \overline{0}$	$\mathbb{Z}$	$\langle\overline{30}\rangle = \langle\overline{0}\rangle$
$\varphi(m) = \overline{m}$	$30\mathbb{Z}$	$\langle\overline{1}\rangle = \mathbb{Z}/30\mathbb{Z}$
$\varphi(m) = \overline{6m}$	$5\mathbb{Z}$	$\langle\overline{6}\rangle$
$\varphi(m) = \overline{10m}$	$3\mathbb{Z}$	$\langle\overline{10}\rangle$
$\varphi(m) = \overline{15m}$	$2\mathbb{Z}$	$\langle\overline{15}\rangle$
$\varphi(m) = \overline{16m}$	$15\mathbb{Z}$	$\langle\overline{16}\rangle = \langle\overline{2}\rangle$
$\varphi(m) = \overline{21m}$	$10\mathbb{Z}$	$\langle\overline{21}\rangle = \langle\overline{3}\rangle$
$\varphi(m) = \overline{25m}$	$6\mathbb{Z}$	$\langle\overline{25}\rangle = \langle\overline{5}\rangle$

□

5. Describe all ring homomorphisms from the ring $\mathbb{Z} \times \mathbb{Z}$ to $\mathbb{Z}$. In each case describe the kernel and the image.

Proof. Let's assume there is a homomorphism φ from $\mathbb{Z} \times \mathbb{Z}$ to $\mathbb{Z}$. Since $\mathbb{Z} \times \mathbb{Z} = \langle(1,0),(0,1)\rangle$ by addition, let's consider the homomorphic images of $(1,0)$ and $(0,1)$ in $\mathbb{Z}$.

Let $\varphi((1,0)) = n$ for some $n \in \mathbb{Z}$, this extends to a homomorphism from $\langle(1,0)\rangle$ to $n\mathbb{Z}$. Since $\langle(1,0)\rangle \cong \mathbb{Z}$, and $\mathbb{Z}$ is homomorphic to $n\mathbb{Z}$ only when $n = 0, 1$, we can determine all the homomorphisms from $\langle(1,0)\rangle$ to $\mathbb{Z}$, namely, $\varphi(s,0) = 0$ and $\varphi(s,0) = s$, where $s \in \mathbb{Z}$. Similarly, the homomorphisms from $\langle(0,1)\rangle$ to $\mathbb{Z}$ are $\varphi(0,r) = 0$ and $\varphi(0,r) = r$, where $r \in \mathbb{Z}$.

For any element $(s,r) \in \mathbb{Z} \times \mathbb{Z}$, $\varphi(s,t) = s \cdot \varphi(1,0) + t \cdot \varphi(0,1)$. Looking through all (four) combinations of the homomorphic images of $\langle(1,0)\rangle$ and $\langle(0,1)\rangle$ we gladly find three of them still remain to be ring homomorphisms. They are:

Homomorphism	Kernel	Image in $\mathbb{Z}$
$\varphi((s,r)) = 0$	$\mathbb{Z} \times \mathbb{Z}$	$\{0\}$
$\varphi((s,r)) = s$	$\{0\} \times \mathbb{Z}$	$\mathbb{Z}$
$\varphi((s,r)) = r$	$\mathbb{Z} \times \{0\}$	$\mathbb{Z}$

□

10. Decide which of the following are ideals of the ring $\mathbb{Z}[x]$.

Proof. (Allman)

(a) The set of all polynomials whose constant term is a multiple of 3. YES.

(b) The set of all polynomials whose coefficient of x^2 is a multiple of 3. NO. Counter-example: $f(x) = 3x^2 + x$ would be in this set, but $f(x) \cdot x = 3x^3 + x^2$ is not. Thus, the 'absorption property' fails.

(c) The set of all polynomials whose constant term, coefficient of x, and coefficient of x^2 are zero. YES. This is the principal ideal generated by x^2, i.e. $I = (x^2)$.

(d) $\mathbb{Z}[x^2]$. NO. The absorption property fails. For instances, $2 \in \mathbb{Z}[x^2]$, but $2x$ is not.

(e) The set of polynomials whose coefficients sum to zero. YES. This is a fancy way of saying that 1 is a root. This set is simply the principal ideal $(x-1)$.

(f) The set of polynomials $p(x)$ such that $p'(0) = 0$, where $p'(x)$ is the usual first derivative of $p(x)$ with respect to x. NO. If $p'(0) = 0$, then x is a root of the derivative of $p(x)$, and any such $p(x)$ has no linear term. That is, if $p(x) = \sum_{i=0}^{k} a_i x^i$, then $a_1 = 0$. This can not be an ideal, since $p(x) = x^2 + 1$ is in this set, but $xp(x) = x^3 + x$ does not satisfy $p'(0) = 0$.

□

17. Let R and S be nonzero rings with identity and denote their respective identities by 1_R and 1_S. Let $\varphi : R \to S$ be a nonzero homomorphism of rings.

(a) Prove that if $\varphi(1_R) \neq 1_S$ then $\varphi(1_R)$ is a zero divisor in S. Deduce that if S is an integral domain then every ring homomorphism from R to S sends the identity of R to the identity of S.

Proof. For φ to be nonzero homomorphism we must have $\varphi(1_R) \neq 0_S$, because if $\varphi(1_R) = 0_S$ then $\forall\ r \in R,\ \varphi(r) = \varphi(1_R \times r) = \varphi(1_R) \times \varphi(r) = 0$. Consider

$$1_S \times \varphi(1_R) = \varphi(1_R) = \varphi(1_R \times 1_R) = \varphi(1_R) \times \varphi(1_R) \Rightarrow (1_S - \varphi(1_R)) \times \varphi(1_R) = 0$$

Now $\varphi(1_R) \neq 0$ and $\varphi(1_R) \neq 1_S$, then $\varphi(1_R)$ must be a zero divisor.

Since integral domains do not allow zero divisors, if S is an integral domain then $\varphi(1_R) = 1_S$, i.e., every ring homomorphism from R to S sends the identity of R to the identity of S. □

(b) Prove that if $\varphi(1_R) = 1_S$ then $\varphi(u)$ is a unit in S and that $\varphi(u^{-1}) = \varphi(u)^{-1}$ for each unit u of R.

Proof. Let u be a unit in $R \Rightarrow \exists\ u^{-1}$ such that $uu^{-1} = u^{-1}u = 1$. Consider $1_S = \varphi(1_R) = \varphi(uu^{-1}) = \varphi(u)\varphi(u^{-1})$, therefore $\varphi(u^{-1}) = \varphi(u)^{-1}$ and $\varphi(u)$ is a unit in S. □

18. a. If I and J are ideals of R prove their intersection $I \cap J$ is also an ideal of R.

Proof. (Baggett) From Exercise 2.1.10(a), $(I \cap J,\ +)$ is a subgroup of $(R,\ +)$ since $(I,\ +)$ and $(J,\ +)$ are subgroups of $(R,\ +)$. Take any element $r \in R$ and any element $k \in I \cap J$. Then $k \in I$ and $k \in J$. Since I and J are ideals, $rk \in I$ and $rk \in J$. Thus, $rk \in I \cap J$. Thus, $I \cap J$ is closed under left multiplication by elements of R. Similarly, $I \cap J$ is closed under right multiplication by elements of R. Hence, $I \cap J$ is an ideal of R. □

b. Prove that the intersection of an arbitrary nonempty collection of ideals is again an ideal (do not assume the collection is countable).

Proof. (Baggett) Let $\{I_\lambda\}_{\lambda \in \Lambda}$ be an arbitrary nonempty collection of ideals of a ring R. From Exercise 2.1.10(b), $(\bigcap_{\lambda \in \Lambda} I_\lambda,\ +)$ is a subgroup of $(R,\ +)$ since for every $\lambda \in \Lambda$, $(I_\lambda,\ +)$ is a subgroup of $(R,\ +)$. Take any element $k \in \bigcap_{\lambda \in \Lambda} I_\lambda$. Then $k \in I_\lambda$ for every $\lambda \in \Lambda$. Since I_λ is an ideal, $rk \in I_\lambda$ for every $\lambda \in \Lambda$. Thus, $rk \in \bigcap_{\lambda \in \Lambda} I_\lambda$. Hence, $\bigcap_{\lambda \in \Lambda} I_\lambda$ is closed under left multiplication by elements of R. Similarly, $\bigcap_{\lambda \in \Lambda} I_\lambda$ is closed under right multiplication by elements of R. Thus, $\bigcap_{\lambda \in \Lambda} I_\lambda$ is an ideal of R. □

22. Let a be an element of the ring R.

a. Prove that $\{x \in R \mid ax = 0\}$ is a right ideal and $\{y \in R \mid ya = 0\}$ is a left ideal (called respectively the right and left annihilators of a in R).

Proof. (Baggett) Let $I = \{x \in R \mid ax = 0\}$ and $J = \{y \in R \mid ya = 0\}$. Take any two elements $x, y \in I$. Then $x - y \in I$ since $a(x - y) = ax - ay = 0$. Thus, $(I,\ +)$ is a subgroup of $(R,\ +)$. Similarly, $(J,\ +)$ is a subgroup of $(R,\ +)$. Take any element $r \in R$ and any element $x \in I$. Then $xr \in I$ since $a(xr) = (ax)r = 0 \cdot r = 0$. Thus, $Ir \subseteq I$ and I is a right ideal. Similarly, take any element $r \in R$ and any element $y \in J$. Then $ry \in J$ since $(ry)a = r(ya) = r \cdot 0 = 0$. Thus, $rJ \subseteq J$ and J is a left ideal. □

b. Prove that if L is a left ideal of R then $\{x \in R \mid xa = 0 \text{ for all } a \in L\}$ is a two-sided ideal (called the left annihilator of L in R).

Proof. (Baggett) Let $I = \{x \in R \mid xa = 0 \text{ for all } a \in L\}$. Take any two elements $x, y \in I$. Then $x - y \in I$ since for any $a \in L$, $(x - y)a = xa - ya = 0$. Thus, $(I, +)$ is a subgroup of $(R, +)$. Take any element $r \in R$ and any element $x \in I$. Then $rx \in I$ since for any $a \in L$, $(rx)a = r(xa) = r \cdot 0 = 0$. Thus, $rI \subseteq I$. Since L is a left ideal of R, $ra \in L$ for every $a \in L$. Let $ra = a' \in L$. Then $xr \in I$ since $(xr)a = x(ra) = xa' = 0$. Thus, $Ir \subseteq I$. Therefore, I is a two-sided ideal. □

24. Let $\varphi : R \to S$ be a ring homomorphism.

    a. Prove that if J is an ideal of S then $\varphi^{-1}(J)$ is an ideal of R. Apply this to the special case when R is a subring of S to deduce that if J is an ideal of S then $J \cap R$ is an ideal of R.

    Proof. (Baggett) Since $(J, +)$ is a subgroup of $(S, +)$ and φ is a group homomorphism under addition, $(\varphi^{-1}(J), +)$ is a subgroup of $(R, +)$ from Exercise 3.1.1. Take any element $r \in R$ and any element $x \in \varphi^{-1}(J)$. Then $rx \in \varphi^{-1}(J)$ since $\varphi(x) \in J$ and $\varphi(rx) = \varphi(r)\varphi(x) \in J$. Similarly, $xr \in \varphi^{-1}(J)$. Thus, $r\varphi^{-1}(J) \subseteq \varphi^{-1}(J)$ and $\varphi^{-1}(J)r \subseteq \varphi^{-1}(J)$. Therefore, $\varphi^{-1}(J)$ is an ideal of R.
    In particular, suppose R is a subring of S and let φ be the inclusion homomorphism, i.e. $\varphi : R \to S$ maps r to r. Let J be an ideal of S. Then $\varphi^{-1}(J) = \{r \in R \mid \varphi(r) \in J\} = \{r \in R \mid r \in J\} = J \cap R$ is an ideal of R. □

    b. Prove that if φ is surjective and I is an ideal of R then $\varphi(I)$ is an ideal of S. Give an example where this fails if φ is not surjective.

    Proof. (Baggett) Since I is an ideal of R, $(I, +)$ is a subgroup of $(R, +)$. Since φ is a group homomorphism under addition, $(\varphi(I), +)$ is a subgroup of $(S, +)$. Take any element $y \in \varphi(I)$ and any element $s \in S$. Since φ is surjective, there exists elements $x \in I$ and $r \in R$ such that $y = \varphi(x)$ and $s = \varphi(r)$. Then $sy \in \varphi(I)$ since $rx \in I$ and $sy = \varphi(r)\varphi(x) = \varphi(rx) \in \varphi(I)$. Similarly, $ys \in \varphi(I)$ as well. Thus, $s\varphi(I) \subseteq \varphi(I)$ and $\varphi(I)s \subseteq \varphi(I)$. Therefore, $\varphi(I)$ is an ideal of S.
    Let $R = \mathbb{Z}$, $S = \mathbb{Q}$, and $\varphi : R \to S$ by $\varphi(n) = n$. Then φ is not surjective. Let $I = 2\mathbb{Z}$. Then $2\mathbb{Z}$ is an ideal of $\mathbb{Z}$; however, $2\mathbb{Z}$ is not an ideal of $\mathbb{Q}$. Take $2 \in 2\mathbb{Z}$ and $\frac{1}{2} \in \mathbb{Q}$. Then $\frac{1}{2} \cdot 2 = 1 \notin 2\mathbb{Z}$. Thus, $\varphi(I) = 2\mathbb{Z}$ is not an ideal of $\mathbb{Q}$. □

Chapter 7.4

4. Assume R is commutative. Prove that R is a field if and only if 0 is a maximal ideal.

Proof (Granade). We shall show each direction in turn.

- $\Rightarrow$ Suppose that R is a field. Then, let I be an ideal of R containing $r \neq 0$. Since R is a field, r^{-1} exists, and so by the absorbing property of I, $1 = r^{-1}r \in I$. But then, for all $s \in R$, we have that $s = s \cdot 1 \in I$ by the same absorbing property. Hence, $I = R$.
- $\Leftarrow$ Suppose that 0 is a maximal ideal in R. Then, fix $r \in R \setminus \{0\}$ and consider the ideal (r). Since 0 is a maximal ideal, we have that $(r) = R$. In particular, $1 \in R$, and so there exists some element $s \in R$ such that $sr = 1$. But then, this gives that $s = r^{-1}$, demonstrating that every element in $R \setminus \{0\}$ has an inverse. We conclude that R is a field.

Since we have shown each direction, we are done. □

5. Prove that if M is an ideal such that R/M is a field, then M is a maximal ideal (do not assume that R is commutative.)

Proof (Granade). Let M be an ideal of R such that R/M is a field. Then, by the Fourth Isomorphism Theorem for Rings, there exists a one-to-one correspondence between ideals $A \supseteq M$ of R and A/M of R/M. But then, by the previous problem, since R/M is a field, it admits only two ideals: R/M and $\{0_{R/M}\}$. Thus, there exists exactly two ideals of R which contain M. We conclude that since M and R are both ideals of R containing M, M is maximal in R. □

11. Assume R is commutative. Let I and J be ideals of R and assume P is a prime ideal of R that contains IJ (for example, if P contains $I \cap J$). Prove either I or J is contained in P.

Proof. (Bastille) By definition $IJ = \{i_1j_1 + i_2j_2 + \cdots + i_nj_n \mid i_k \in I, j_k \in J, n \in \mathbb{Z}^+\}$. If $J \subseteq P$ then we are done so assume J is not contained in P. Then there exists $j \in J$ such that $j \notin P$. Let $i \in I$. Then $ij \in P$ since $\{ij \mid i \in I\} \subseteq IJ \subseteq P$, but then since P is a prime ideal, we must have $i \in P$. Therefore $I \subseteq P$. Thus in every case, either I or J is contained in P. □

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.

(a) *Proof.* (Bastille) Let P be a prime ideal of S. By Exercise 7.3.24(a), since P is an ideal of S, then $\varphi^{-1}(P)$ is an ideal of R. If $\varphi^{-1}(P) = R$ then we are done. So assume $\varphi^{-1}(P) \neq R$ and let $ab \in \varphi^{-1}(P)$. Then $\varphi(ab) = \varphi(a) \cdot \varphi(b) \in P$ and so either $\varphi(a)$ or $\varphi(b)$ is in P since P is a prime ideal. Hence by definition of $\varphi^{-1}(P)$, either a or b is in $\varphi^{-1}(P)$. Therefore, $\varphi^{-1}(P)$ is a prime ideal of R. □

Remark Let R be a subring of S, let φ be the inclusion homomorphism, i.e. $\varphi : R \to S$ is defined by $\varphi(r) = r$, and let P be a prime ideal of S. By definition,

$$\varphi^{-1}(P) = \{r \in R \mid \varphi(r) \in P\} = \{r \in R \mid r \in P\} = P \cap R.$$

Hence by the Proposition above, $P \cap R = R$ or $P \cap R$ is a prime ideal of R.

(b) *Proof.* (Bastille) Let M be a maximal ideal of S and let φ be a surjective homomorphism from R to S. Since M is maximal, it is prime, and so by part (a), $\varphi^{-1}(M)$ is either R or a prime ideal of R. We claim that since φ is surjective we cannot have $\varphi^{-1}(M) = R$. Assume to the contrary that $\varphi^{-1}(M) = R$. Then because φ is surjective,

$$M = \varphi(\varphi^{-1}(M)) = \varphi(R) = S.$$

Yet M is a maximal ideal of S so $M \neq S$ and we have reached a contradiction. So we can now proceed assuming $\varphi^{-1}(M)$ is a prime ideal of R. Define the following map:

$$\sigma : R \to S/M$$
$$\sigma(r) = \varphi(r) + M.$$

We verify that σ is well-defined and a ring homomorphism since

$$\begin{aligned}\forall\, r_1, r_2 \in R: \quad \sigma(r_1 + r_2) &= \varphi(r_1 + r_2) + M \\ &= \varphi(r_1) + \varphi(r_2) + M \quad \text{since } \varphi \text{ is a ring homomorphism} \\ &= (\varphi(r_1) + M) + (\varphi(r_2) + M) \quad \text{since } M \text{ is an ideal} \\ &= \sigma(r_1) + \sigma(r_2), \\ \text{and} \quad \sigma(r_1 r_2) &= \varphi(r_1 r_2) + M \\ &= \varphi(r_1)\varphi(r_2) + M \quad \text{since } \varphi \text{ is a ring homomorphism} \\ &= (\varphi(r_1) + M)(\varphi(r_2) + M) \quad \text{since } M \text{ is an ideal} \\ &= \sigma(r_1)\sigma(r_2).\end{aligned}$$

Furthermore,

$$\ker \sigma = \{r \in R \mid \varphi(r) + M = M\} = \{r \in R \mid \varphi(r) \in M\} = \varphi^{-1}(M),$$

and the map is surjective since φ is surjective. Therefore, by the First Isomorphism Theorem,

$$R/\varphi^{-1}(M) \cong S/M.$$

But because M is maximal in S, S/M is a field. Therefore, $R/\varphi^{-1}(M)$ is a field, and consequently $\varphi^{-1}(M)$ is maximal. □

Remark This need not be true if φ is not surjective. Let M be a maximal ideal of S, let $R = M$ and define φ as the inclusion map, $\varphi : R \to S$, $\varphi(r) = r$. Then $\varphi^{-1}(M) = R$, which is not a maximal ideal of R since it equals R. Concretely, consider $\varphi : 2\mathbb{Z} \to \mathbb{Z}$, $\varphi(k) = k$, $M = 2\mathbb{Z}$, a maximal ideal in $\mathbb{Z}$, yet since $\varphi^{-1}(2\mathbb{Z}) = 2\mathbb{Z}$, it is not a maximal ideal of $2\mathbb{Z}$.

25. Assume R is commutative and for each $a \in R$ there is an integer $n > 1$ such that $a^n = a$. Prove that every prime ideal of R is maximal.

Proof. (Lawless) Let P be a prime ideal of R. Since R is commutative, then we know R/P will be an integral domain. We will show R/P is a field.

Let $a + P \neq 0 + P$, and fix $n \in \mathbb{Z}^+$ so that $a^n = a$. Notice

$$(a + P)(a^{n-1} + P) = a^n + P = a + P.$$

Therefore,

$$\begin{aligned}0 + P &= (a + P)(a^{n-1} + P) - (a + P) \\ &= (a + P)[(a^{n-1} + P) - (1 + P)]\end{aligned}$$

Since P is a prime ideal, and we assumed $a + P \neq P$, then $(a^{n-1} + P) - (1 + P) = P$. Thus, $a^{n-1} + P = 1 + P$. Therefore $(a + P)(a^{n-2} + P) = 1 + P$. Therefore, $a + P$ is a unit, and so R/P is a field. So P is a maximal ideal. □

27. Let R be a commutative ring with unity. Prove that if a is a nilpotent element of R, then $1 - ab$ is a unit for all $b \in R$.

Proof. (Lawless) Let $a \in R$ satisfy $a^n = 0$. Then for any $b \in R$,

$$\begin{aligned}(1 - ab)(1 + ab + (ab)^2 + \ldots + (ab)^{n-1}) &= 1 - (ab)^n \\ &= 1 - a^n b^n \text{ (since } R \text{ is commutative)} \\ &= 1.\end{aligned}$$

Therefore, $(1 - ab)^{-1} = \sum_{k=0}^{n-1} (ab)^k$, and so $(1 - ab)$ is a unit in R.

□