Homework 3 Solutions.

§5.3, #7 Show that the intersection of two ideals of a commutative ring is again an ideal.

Proof. Let $I, J \lhd R$ with R a commutative ring. Let $a, b \in I \cap J$. Then we have $a, b \in I$ and $a, b \in J$. Since $I, J \lhd R$, we have $a \pm b \in I \cap J$ and $ab \in I \cap J$. It follows that $I \cap J \lhd R$. □

§5.3, #8 Show that if R is a finite ring, then every prime ideal of R is maximal.

Proof. Let R be a finite ring and let $P \lhd R$ be a prime ideal. Since P is prime, the quotient R/P is an integral domain; since R is finite, the quotient is finite. Hence, R/P is a finite integral domain. As such, it is a field, and therefore, P is maximal. □

§5.3, #9 Find a non-zero prime ideal of $\mathbb{Z} \oplus \mathbb{Z}$ that is not maximal.

Solution: We claim that $I = \{(0, n) : n \in \mathbb{Z}\}$ is a prime ideal of $\mathbb{Z} \oplus \mathbb{Z}$ which is not maximal. To see that it is an ideal, note that for all $(0, n_1)$, $(0, n_2) \in I$, we have $(0, n_1) \pm (0, n_2) = (0, n_1 \pm n_2) \in I$. Furthermore, for $(r_1, r_2) \in \mathbb{Z} \oplus \mathbb{Z}$ and $(0, n) \in I$, we have $(r_1, r_2) \cdot (0, n) = (0, r_2 n) \in I$. Now, we claim that $(\mathbb{Z} \oplus \mathbb{Z})/I \cong \mathbb{Z}$. For this, we define a map $\phi : \mathbb{Z} \oplus \mathbb{Z} \to \mathbb{Z}$ by $\phi((n_1, n_2)) = n_1$. We observe that $\phi((1, 1)) = 1$ and that $\phi((n_1, n_2) + (r_1, r_2)) = \phi((n_1 + r_1, n_2 + r_2)) = n_1 + r_1 = \phi((n_1, n_2)) + \phi((r_1, r_2))$. We also see that $\phi((n_1, n_2)(r_1, r_2)) = \phi((n_1 r_1, n_2 r_2)) = n_1 r_1 = \phi((n_1, n_2))\phi((r_1, r_2))$. Therefore, ϕ is an onto homomorphism with $\ker\phi = I$. Applying the fundamental homomorphism theorem for rings yields $(\mathbb{Z} \oplus \mathbb{Z})/I \cong \mathbb{Z}$. Since $\mathbb{Z}$ is an integral domain, but not a field, it follows that I is prime, but not maximal.

§5.3, #11 Let R be a commutative ring with $a \in R$. The **annihilator** of a is defined by $\text{Ann}(a) = \{x \in R : xa = 0\}$. Prove that $\text{Ann}(a)$ is an ideal of R.

Proof. Let $x_1, x_2 \in \text{Ann}(a)$. Then we have $x_1 a = 0$ and $x_2 a = 0$. It follows that $(x_1 \pm x_2)a = x_1 a \pm x_2 a = 0 \pm 0 = 0$. Hence, we have $x_1 \pm x_2 \in \text{Ann}(a)$. But also, for $x \in \text{Ann}(a)$ and $r \in R$, we have $(rx)a = r(xa) = r \cdot 0 = 0$ from which it follows that $rx \in \text{Ann}(a)$. Therefore, $\text{Ann}(a)$ is an ideal of R. □

§5.3, #12 (a) Show that the set $N = \{a \in R : \exists n \geq 1 \text{ with } a^n = 0\}$ of all nilpotent elements of a commutative ring forms an ideal of the ring.

Proof. Let $a, b \in N$. Then there are $n_1, n_2 \geq 1$ with $a^{n_1} = b^{n_2} = 0$. Let $n = \max(n_1, n_2)$. Then we have $a^n = b^n = 0$. Since R is commutative, the binomial theorem holds, which we apply to $(a \pm b)^{2n}$:

$$(a \pm b)^{2n} = \sum_{i=0}^{2n} \binom{2n}{i} a^i (-b)^{2n-i} = 0$$

since each summand has one of i and $2n - i \geq n$. It follows that $a \pm b \in N$. Now, let $r \in R$. Since R is commutative, we have $(ra)^n = r^n a^n = r^n \cdot 0 = 0$. Therefore, we have $ra \in N$. Hence, we have $N \lhd R$. □

(b) Show that R/N hs no non-zero nilpotent elements.

Proof. Observe that $(a+N)^n = N$ in R/N if and only if $a^n + N = N$, which holds if and only if $b = a^n \in N$. Now, $b \in N$ implies that there is an $m \geq 1$ with $b^m = (a^n)^m = a^{nm} = 0$. Therefore, we have $a \in N$. It follows that R/N has no nilpotent elements. $\square$

(c) Show that $N \subseteq P$ for each prime ideal P of R.

Proof. Let $a \in N$ and let $P \triangleleft R$ be prime. Then there is a smallest $n \geq 1$ with $a^n = 0$. Observe that $a^n = 0 \in P$. Since P is prime, we must have $a \in P$. $\square$

§5.3, #13 Let R be a commutative ring with ideals I, J. Let

$$I + J = \{x \in R : x = a + b \text{ for some } a \in I, b \in J\}.$$

(a) Show that $I + J$ is an ideal.

Proof. Let $x_1 = i_1 + j_1, x_2 = i_2 + j_2 \in I + J$. Then we have $x_1 \pm x_2 = (i_1 \pm i_2) + (j_1 \pm j_2) \in I + J$ since $i_1 \pm i_2 \in I$ and $j_1 \pm j_2 \in J$. It follows that $x_1 \pm x_2 \in I + J$. Now, let $x = i + j \in I + J$ and let $r \in R$. Then we have $rx = ri + rj \in I + J$ since $ri \in I$ and $rj \in J$. It follows that $rx \in I + J$ and that $I + J$ is an ideal of R. $\square$

(b) Determine $n\mathbb{Z} + m\mathbb{Z}$ in the ring of integers.

Solution: We have $n\mathbb{Z} + m\mathbb{Z} = \gcd(m, n)\mathbb{Z}$. For a proof, see Theorem 1.1.6 on p. 8 of the text.

§5.3, #14 Let R be a commutative ring with ideals I, J. Define the product of the two ideals by

$$IJ = \left\{ \sum_{i=1}^{n} a_i b_i : a_i \in I, b_i \in J, n \in \mathbb{N} \right\}.$$

(a) Show that IJ is an ideal contained in $I \cap J$.

Proof. Let $x = \sum_{i=1}^{n} a_i b_i$, $y = \sum_{j=1}^{m} c_j d_j$. Then we have

$$x \pm y = \sum_{i=1}^{n} a_i b_i \pm \sum_{j=1}^{m} c_j d_j = \sum_{i=1}^{n} a_i b_i + \sum_{j=1}^{m} (\pm c_j) d_j \in IJ$$

since it is a finite sum ($n + m$ summands) with summands obtained as products of elements from I with elements from J. Now, let $r \in R$. Then we have

$$rx = \sum_{i=1}^{n} (ra_i) b_1 \in IJ$$

since $ra_i \in I$. It follows that $IJ \triangleleft R$. Moreover, observe that $x = \sum a_i b_i \in I$ since $a_i \in I$, $b_i \in R$, and $I \triangleleft R$. Similarly, $x \in J$ since $a_i \in R$, $b_i \in J$, and $J \triangleleft R$. Hence, we must have $IJ \subseteq I \cap J$.

$\square$

(b) Determine $(n\mathbb{Z})(m\mathbb{Z})$ in the ring of integers.

Solution: We claim that $(n\mathbb{Z})(m\mathbb{Z}) = (nm)\mathbb{Z}$. To see this, let $x \in (n\mathbb{Z})(m\mathbb{Z})$. Then there are r_i, $r_i' \in \mathbb{Z}$ for which $x = \sum_{i=1}^{n}(r_i n)(r_i' m) = nm\sum_{i=1}^{n} r_i r_i' \in (nm)\mathbb{Z}$. It follows that $(n\mathbb{Z})(m\mathbb{Z}) \subseteq (nm)\mathbb{Z}$. On the other hand if $y \in (nm)\mathbb{Z}$, then there is an $r \in \mathbb{Z}$ with $y = rnm = (rn)m \in (n\mathbb{Z})(m\mathbb{Z})$ since $rn \in n\mathbb{Z}$. Thus, we have $y \in (n\mathbb{Z})(m\mathbb{Z})$.

§5.3, #17 b, c Let R be the set of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with entries a, b, c, $d \in \mathbb{Q}$ such that $a = d$ and $c = 0$.

(b) Let I be the set of all matrices for which $a = d = 0$. Show that I is an ideal of R.

Proof. Let $X = \begin{pmatrix} 0 & b_1 \\ 0 & 0 \end{pmatrix}$, $Y = \begin{pmatrix} 0 & b_2 \\ 0 & 0 \end{pmatrix} \in I$, and let $Z = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in R$. Then we have

$$X \pm Y = \begin{pmatrix} 0 & b_1 \pm b_2 \\ 0 & 0 \end{pmatrix} \in I, \quad ZX = \begin{pmatrix} 0 & ab_1 \\ 0 & 0 \end{pmatrix} \in I, XZ = \begin{pmatrix} 0 & ab_1 \\ 0 & 0 \end{pmatrix} \in I.$$

Hence, I is an ideal in R. □

(c) Use the fundamental homomorphism theorem for rings to show that $\mathbb{R}/I \cong \mathbb{Q}$.

Proof. Define a map $\phi : R \to \mathbb{Q}$ by $\phi\left(\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}\right) = a$. We claim that ϕ is a ring homomorphism. First, we observe that $\phi\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) = 1$. Let $A = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$, $B = \begin{pmatrix} c & d \\ 0 & c \end{pmatrix} \in R$. We have

$$\phi\left(\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}\begin{pmatrix} c & d \\ 0 & c \end{pmatrix}\right) = \phi\left(\begin{pmatrix} ac & ad+bc \\ 0 & ac \end{pmatrix}\right) = ac = \phi\left(\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}\right)\phi\left(\begin{pmatrix} c & d \\ 0 & c \end{pmatrix}\right)$$
$$\phi(\left(\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} + \begin{pmatrix} c & d \\ 0 & c \end{pmatrix}\right) = \phi(\left(\begin{pmatrix} a+c & b+d \\ 0 & a+c \end{pmatrix}\right) = a+c = \phi\left(\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}\right) + \phi\left(\begin{pmatrix} c & d \\ 0 & c \end{pmatrix}\right).$$

Therefore, ϕ is an onto ring homomorphism with kernel I. The fundamental ring homomorphism theorem gives $R/I \cong \mathbb{Q}$. □

§5.3, #20 Let p be prime and let $(p) \triangleleft \mathbb{Z}[i] = R$. Show that $R/(p)$ has p^2 elements and characteristic p.

Proof. Consider the map $\phi : R \to \mathbb{Z}_p \oplus \mathbb{Z}_p$ defined by $\phi(a+bi) = ([a]_p, [b]_p)$. We claim that this map is a homomorphism of **groups**. Let $a+bi$, $c+di \in R$. Then we have $\phi((a+bi)+(c+di)) = \phi((a+c)+(b+d)i) = ([a+c]_p, [b+d]_p) = ([a]_p, [b]_p)+([c]_p, [d]_p) = \phi(a+bi)+\phi(c+di)$. It follows that ϕ is an group homomorphism with kernel (p); by the fundamental group homomorphism theorem we see that $R/(p) \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$ as groups. Hence, we see that $|R/(p)| = p^2$. Moreover, we see that $R/(p) = \{a+bi+(p) : 0 \le a, b \le p-1\}$.

It remains to verify that the characteristic of the quotient is p. We observe that $p(1+(p))p + (p) = 0 + (p)$ and that p is the smallest positive integer r for which $r(1+(p)) = (p)$. □

§5.3, #21 Let $R = \mathbb{Z}[i]$. Find necessary and sufficient conditions on $m, n \in \mathbb{Z}$ for the element $m + ni$ to belong to the ideal $(1 + 2i)$. Use these conditions to determine the ideal $(1 + 2i) \cap \mathbb{Z} \triangleleft \mathbb{Z}$.

Solution: We observe that $m + ni \in (2 + i)$ if and only if $\exists a + bi \in R$ with $m + ni = (a + bi)(2 + i) = (a - 2b) + (2a + b)i$. Hence, we see that $m + ni \in R$ if and only if $\exists a$, $b \in \mathbb{Z}$ with $m = a - 2b$ and $n = 2a + b$. Therefore, we have $m + ni \in (1 + 2i) \cap \mathbb{Z}$ if and only if $n = 2a + b = 0$, in which case $b = -2a$ and $m = a - 2b = a - 2(-2a) = 5a$. It follows that $(1 + 2i) \cap \mathbb{Z} = 5\mathbb{Z}$.

§5.3, #26, b, c, d, e (b) Show that (2^k) is an ideal of R.

Proof. This is is the principal ideal generated by 2^k. It is proper since $1 \notin (2^k)$. (If $1 \in (2^k)$, then there is $m/n \in R$ with $1 = 2^k(m/n)$; hence, we have $2^k \mid n$, a contradiction since n is odd. On the other hand, if $m \in \mathbb{Z}$ is odd, we have $(m) = (1) = R$ since $1 = m(1/m)$. □

(c) Show that every proper non-zero ideal of R has the form (2^k) for some $k \geq 1$.

Proof. Express $m/n \in R$ as $m/n = (2^t a)/b$ for some $t \in \mathbb{Z}$ and odd a, b. We define $v_2(m/n) = t$. It follows that $R = \{m/n \in \mathbb{Q} : v_2(m/n) \geq 0\}$. Now, let $I \triangleleft R$ be proper. We first claim that for all $m/n \in I$, we have $v_2(m/n) \geq 1$. If not, then for some $m/n \in I$, we have $v_2(m/n) = 0$, which implies that m is odd. Therefore, we have $n/m \in R$ and $(m/n)(n/m) = 1 \in I$, so $I = R$, a contradiction.

Hence, we let $k = \min(v_2(m/n) : m/n \in I\} \geq 1$. By the argument above, such a k exists. Let $m_0/n_0 \in I$ have $v_2(m_0/n_0) = k$. Then we write $m_0/n_0 = (2^k a_0)/b_0$ with odd a_0, b_0. We now assert that $I = (2^k)$. Let $m/n \in I$. Then we have $v_2(m/n) = k_1 \geq k$; it follows that $m/n = (2^{k_1} a)/b$ with odd a, b. We observe that $m/n = 2^k((2^{k_1 - k} a)/b) \in (2^k)$. Hence, we have $I \subseteq (2^k)$. Next, note that $2^k = (m_0/n_0)(b_0/a_0) \in I$ since $m_0/n_0 \in I$ and $b_0/a_0 \in R$, which gives $(2^k) \subseteq I$.

□

(d) Show that $R/(2^k) \cong \mathbb{Z}_{2^k}$.

Proof. Define a map $\phi : R \to \mathbb{Z}_{2^k}$ by $\phi(m/n) = [mn^{-1}]_{2^k}$. This is an onto ring homomorphism with kernel (2^k). The result follows from the fundamental ring homomorphism theorem. □

(e) Show that (2) is the unique maximal ideal in R.

Proof. Let $I \triangleleft R$ be a non-zero ideal of R. Parts (b), (c), (d) show that R/I is a field if and only if $I = (2)$. Therefore, I is the only maximal ideal in R. □