Chapter 1

Commutative Rings

Definitions

1. prime, coprime, relatively prime, irreducible

Exercise 1.1. Let $\varphi : A \longrightarrow B$ be a ring homomorphism, $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3$ ideals in A, and $\mathfrak{b}_1, \mathfrak{b}_2, \mathfrak{b}_3$ ideals of B. Prove the following statements.

1. $(\mathfrak{a}_1 + \mathfrak{a}_2)^e = (\mathfrak{a}_1)^e + (\mathfrak{a}_2)^e$.

   Proof. We show $(\mathfrak{a}_1 + \mathfrak{a}_2)^e \subseteq (\mathfrak{a}_1)^e + (\mathfrak{a}_2)^e$. Let $x \in (\mathfrak{a}_1 + \mathfrak{b}_2)^e$, then we have for some index set I

   $$x = \sum_{i \in I} \lambda_i x_i, \tag{1.1}$$

   where $\lambda_i \in B$ and $x_i \in \varphi(\mathfrak{a}_1 + \mathfrak{a}_2)$ for all $i \in I$. For each $i \in I$ it is $x_i = \varphi(\mu_{i,1} a_{i,1} + \mu_{i,2} a_{i,2})$, hence

   $$\begin{aligned}
   x =& \sum_{i \in I} \lambda_i \varphi(\mu_{i,1} a_{i,1} + \mu_{i,2} a_{i,2}) && (1.2)\\
   =& \sum_{i \in I} \lambda_i \left(\varphi(\mu_{i,1} a_{i,1}) + \varphi(\mu_{i,2} a_{i,2})\right) \qquad \text{(by linearity)} && (1.3)\\
   =& \sum_{i \in I} \lambda_i \left(\mu_{i,1}\varphi(a_{i,1}) + \mu_{i,2}\varphi(a_{i,2})\right) \qquad \text{(by linearity)} && (1.4)\\
   =& \sum_{i \in I} \lambda_i \mu_{i,1}\varphi(a_{i,1}) + \lambda_i \mu_{i,2}\varphi(a_{i,2}) \qquad \text{(by distributivity)} && (1.5)\\
   =& \sum_{i \in I} \lambda_i \mu_{i,1}\varphi(a_{i,1}) + \sum_{i \in I} \lambda_i \mu_{i,2}\varphi(a_{i,2}) \qquad \text{(reordering the sum).} && (1.6)\\
   & && (1.7)
   \end{aligned}$$

   The last term is exactly the elements expressed by $\mathfrak{a}_1^e + \mathfrak{a}_2^e$, therefore, $(\mathfrak{a}_1 + \mathfrak{a}_2)^e \subseteq (\mathfrak{a}_1)^e + (\mathfrak{a}_2)^e$.
   I think the above proof should work into both directions. □

2. $(\mathfrak{b}_1 + \mathfrak{b}_2)^c \supseteq \mathfrak{b}_1^c + \mathfrak{b}_2^c$

   Proof. We have

   $$(\mathfrak{b}_1 + \mathfrak{b}_2)^c = \left\{ x \in A \;\middle|\; \exists b_1 \in \mathfrak{b}_1 \exists b_2 \in \mathfrak{b}_2 : \varphi(x) = b_1 + b_2 \right\}. \tag{1.8}$$

   Now let $x \in \mathfrak{b}_1^c + \mathfrak{b}_2^c$, then $x = a_1 + a_2$ where $\varphi(a_1) \in \mathfrak{b}_1$ and $\varphi(a_2) \in \mathfrak{b}_2$. It is

   $$\begin{aligned}
   \varphi(x) =& \varphi(a_1 + a_2) && (1.9)\\
   =& \varphi(a_1) + \varphi(a_2) \qquad \text{(by additivity)} && (1.10)
   \end{aligned}$$

   Since $\varphi(a_1) \in \mathfrak{b}_1$ and $\varphi(a_2) \in \mathfrak{b}_2$ we have that $x \in (\mathfrak{b}_1 + \mathfrak{b}_2)^c$. □

Exercise 1.2. Let $\varphi : A \longrightarrow B$ be a ring homomorphism, $\mathfrak{a}$ an ideal of A, and $\mathfrak{b}$ an ideal of B. Prove the following statements:

1. Then $\mathfrak{a} \subseteq \mathfrak{a}^{ec}$.

Proof. It is

$$\mathfrak{a}^{ec} = \left\{ x \in A \,\middle|\, \varphi(x) \in \mathfrak{a}^e \right\} \tag{1.11}$$
$$= \left\{ x \in A \,\middle|\, \varphi(x) \in \langle \varphi(\mathfrak{a}) \rangle \right\} \tag{1.12}$$
$$= \left\{ x \in A \,\middle|\, \forall i \in I\, \exists a_i \in \mathfrak{a}_1 : \varphi(x) = \sum_{i \in I} \lambda_i \varphi(a_i) \right\}. \tag{1.13}$$

Let $a \in \mathfrak{a}$ and choose $I = \{ 1 \}$, λ_1, and $a_i = a$, then $a \in \mathfrak{a}^{ec}$. ☐

2. $\mathfrak{b}^{ce} \subseteq \mathfrak{b}$.
3. $\mathfrak{a}^{ece} = \mathfrak{a}^e$.
4. $\mathfrak{b}^{cec} = \mathfrak{b}^c$.
5. If $\mathfrak{b}$ is an extension, then $\mathfrak{b}^c$ is the largest ideal of A with extension $\mathfrak{b}$.
6. If two extensions have the same contraction, then they are equal.

   Proof. a ☐

Exercise 1.3. Let A be a ring, $A[\mathcal{X}, \mathcal{Y}]$ the polynomial ring in two sets of variables $\mathcal{X}$ and $\mathcal{Y}$. Show that $\langle \mathcal{X} \rangle$ is prime if and only if A is a domain.

Proof. It should be noted here, that $A[\mathcal{X}]$ does not contain $X_1 X_2$ for example. It does contain $X_1 + X_2$ however. The rest is easy. ☐

Exercise 1.4. Show that, in a PID, nonzero elements x and y are relatively prime (share no prime factor) if and only if they're coprime.

Exercise 1.5. Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals, and $\mathfrak{p}$ a prime ideal. Prove that these conditions are equivalent:

1. $\mathfrak{a} \subseteq \mathfrak{p}$ or $\mathfrak{b} \subseteq \mathfrak{p}$
2. $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{p}$
3. $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$

Proof. (1) to (2) is easy. Same for (2) to (3). For (3) to (1) show it with contradiction. ☐

Exercise 1.6. Let A be a ring, $\mathfrak{p}$ a prime ideal, and $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ maximal ideals with $\mathfrak{m}_1, \ldots, \mathfrak{m}_n = 0$. Show $\mathfrak{p} = \mathfrak{m}_i$ for some i.

Proof. By induction. Proof first for $m_1 m_2$, the rest is clear. ☐

Exercise 1.7. Let A be a ring, $\mathfrak{p}$ a prime, and $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ ideals.

1. If $\bigcap_{i=1}^n \mathfrak{a}_i \subseteq \mathfrak{p}$, then $\mathfrak{a}_j \subseteq \mathfrak{p}$ for some j.

   Proof. If $\mathfrak{a}_1 \cap \mathfrak{a}_2 \subseteq \mathfrak{p}$, then by the exercise above we have the desired result. The rest is induction. ☐

2. If $\bigcap_{i=1}^n \mathfrak{a}_i = \mathfrak{p}$, then $\mathfrak{a}_j \subseteq \mathfrak{p}$ for some j.

   Proof. Clear. ☐

Exercise 1.8. Let A be a ring, $\mathcal{S}$ the set of all ideals that consist entirely of zerodivisors. Show that $\mathcal{S}$ has maximal elements and they're prime. Conclude that $\mathrm{ZD}(A)$ is a union of primes.

Exercise 1.9. Exercise 2.27, proof is silly

Exercise 1.10. Let $A_1 \times A_2$ be a product of two rings. Show that $A_1 \times A_2$ is a domain if and only if either A_1 or A_2 is a domain and the other is 0.

Proof. The back implication is clear.
For the other implication, assume neither is integral domain, this leads to an obvious contradiction.
Now assume neither is 0. Choose $(a, 0) and (0, b)$, contradiction. ☐

Exercise 1.11. Let $A_1 \times A_2$ be a product of rings, $\mathfrak{p} \subset A_1 \times A_2$ an ideal. Show that $\mathfrak{p}$ is prime if and only if either $\mathfrak{p} = \mathfrak{p}_1 \times A_2$ with $\mathfrak{p}_1 \subseteq A_1$ prime or $\mathfrak{p} = A_1 \times \mathfrak{p}_2$ with $\mathfrak{p}_2 \subseteq A_2$ prime.

Proof. If $\mathfrak{p}$ is prime, then for each $(x, y) \in \mathfrak{p}$ we have that $(x, 1) \in \mathfrak{p}$ or $(1, y) \in \mathfrak{p}$. From this the first implication follows.

For the other side is clear. □

Exercise 1.12. Let A be a domain, and $x, y \in A$ with $\langle x \rangle = \langle y \rangle$. Show $x = uy$ for some unit u.

Proof. From $\langle x \rangle = \langle y \rangle$ we get that $rx = sy$ for some $r, s \in A$. Because A is a domain, we have $\frac{r}{s} x = y$. This is a unit because $\frac{r}{s} \cdot \frac{s}{r} = 1$. □

Exercise 1.13. Let k be a field, R a nonzero ring, $\varphi : k \longrightarrow R$ a ring map. Prove φ is injective.

Proof. The trick here is to know that the kernel is an ideal. Since the kernel contains 0, it must also contain the ideal generated by it. Now, in all fields is the zeroideal maximal, hence the kernel is already maximal and contains only 0. From that we conclude φ is injective. □

Exercise 1.14. Let A be a ring, $\mathfrak{p}$ a prime, $\mathcal{X}$ a set of variables. Let $\mathfrak{p}[\mathcal{X}]$ denote the set of polynomials with coefficients in $\mathfrak{p}$. Prove these statements:

1. $\mathfrak{p}R[\mathcal{X}]$ and $\mathfrak{p}[\mathcal{X}]$ and $\mathfrak{p}R[\mathcal{X}] + \langle \mathcal{X} \rangle$ are primes of $R[\mathcal{X}]$, which contract to $\mathfrak{p}$.

   Proof. We have $R[\mathcal{X}] \big/ \mathfrak{p}R[\mathcal{X}] \simeq \left(R/\mathfrak{p} \right) [\mathcal{X}]$. The latter one is a domain because it is the polynomial ring of a domain. Therefore, $\mathfrak{p}R[\mathcal{X}]$ is prime.

   We also have $\mathfrak{p}R[\mathcal{X}] = \mathfrak{p}[\mathcal{X}]$.

   For the contraction let $\varphi : R \longrightarrow R[\mathcal{X}]$. Then $\varphi^{-1}(\mathfrak{p}[\mathcal{X}]) = \mathfrak{p}$.

   For the last part, consider
   $$\varphi : R[\mathcal{X}] \longrightarrow R/\mathfrak{p} \tag{1.14}$$
   with the natural definition $\varphi(a_0 + a_1 X + \ldots + a_n X^n) = a_0 + \mathfrak{p}$. Then, the kernel is all the polynomials with $a_0 \in \mathfrak{p}$ so $\mathfrak{p}R[\mathcal{X}] + \langle \mathcal{X} \rangle$. Since φ is obviously surjective, we have the isomorphism
   $$R[\mathcal{X}] \big/ \mathfrak{p}R[\mathcal{X}] + \langle \mathcal{X} \rangle \simeq R/\mathfrak{p} \tag{1.15}$$
   The latter is a domain, so is the former, hence $\mathfrak{p}R[\mathcal{X}] + \langle \mathcal{X} \rangle$ is prime.

   Again for the contraction we have $\varphi^{-1}(\mathfrak{p}R[\mathcal{X}] + \langle \mathcal{X} \rangle) = \mathfrak{p}$ (because we are basically only caring about a_0). □

2. Assume $\mathfrak{p}$ is maximal. Then $\mathfrak{p}R[\mathcal{X}] + \langle \mathcal{X} \rangle$ is maximal.

   Proof. From above, we have an isomorphism
   $$R[\mathcal{X}] \big/ \mathfrak{p}R[\mathcal{X}] + \langle \mathcal{X} \rangle \simeq R/\mathfrak{p} \tag{1.16}$$
   therefore, if $\mathfrak{p}$ is maximal so is $\mathfrak{p}R[\mathcal{X}] + \langle \mathcal{X} \rangle$. □

Exercise 1.15. Let R be a ring, X a variable, $H \in P := R[X]$, and $a \in R$. Given $n \geq 1$, show $(X - a)^n$ and H are coprime if and only if $H(a)$ is a unit.