

Exercises 7, 11, 13, 14, 16, 30, 31 (except (e)), pp. 256-260.

Let R be a ring with identity $1 \neq 0$.

Problem 7. Let R be a commutative ring with 1. Prove that the principal ideal generated by x in the polynomial ring $R[x]$ is a prime ideal if and only if R is an integral domain. Prove that (x) is a maximal ideal if and only if R is a field.

Proof. The ideal (x) is prime if $ab \in (x) \Rightarrow a \in (x) \vee b \in (x)$ by definition. We apply the equivalence that $r \in (x) \iff \bar{r} = \bar{0} \in R[x]/(x)$. Thus the definition (x) being prime is equivalent to $\overline{ab} = \bar{a}\bar{b} = \bar{0} \Rightarrow \bar{a} = \bar{0} \vee \bar{b} = \bar{0}$, i.e. $R[x]/(x)$ is an integral domain. \square

Problem 11. Assume R is commutative. Prove that if P is a prime ideal of R and P contains no zero divisors then R is an integral domain.

Proof. Let $a, b \in R$ be any elements such that $ab = 0$. Note that $ab \in P$, and since P is prime, we have that either $a \in P$ or $b \in P$. Suppose $a \in P$. Then since P has no zero-divisors, $ab = 0$ forces $a = 0$. The same argument applies when $b \in P$ to show that $b = 0$. In any case, either $a = 0$ or $b = 0$. Hence R is an integral domain. \square

Problem 13. Let $\varphi : R \rightarrow S$ 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 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.

Proof. We proceed with each separately:

- (a) Let $P \leq S$ be a prime ideal. We can split into two cases: $\varphi^{-1}(P) = R$ or $\varphi^{-1}(P) < R$.

In the first case, we're just done.

In the second case, let $a, b \in R$ and $ab \in \varphi^{-1}(P)$. Then we can do some map manipulations to see that

$$\varphi(ab) = \varphi(a)\varphi(b) \in P \Rightarrow \varphi(a) \in P \vee \varphi(b) \in P \Rightarrow a \in \varphi^{-1}(P) \vee b \in \varphi^{-1}(P),$$

where the first implication is due to the fact that S is integral. Hence we have both conditions, so $\varphi^{-1}(P)$ is integral.

In the special case where we consider the inclusion $\iota : R \hookrightarrow S$, we have $\varphi^{-1}(P) = P \cap R$; so $P \cap R$ is either R or a prime ideal of R .

- (b) Let I be any ideal such that $\varphi^{-1}(M) \leq I \leq R$. Then we have $M \leq \varphi(I) \leq \varphi(R)$. Since φ is surjective, we may identify $\varphi(R) = S$. Since M is maximal, we deduce that $\varphi(I)$ must be either M or S . Thus I must be either $\varphi^{-1}(M)$ or $\varphi^{-1}(S) = R$, which means exactly that $\varphi^{-1}(M)$ is maximal.

□

Problem 14. TODO

Proof. **TODO**

□

Problem 16. Let $x^2 - 16$ be an element of the polynomial ring $E = \mathbb{Z}[x]$ and use the bar notation to denote passage to the quotient ring $\mathbb{Z}[x]/(x^3 - 2x + 1)$. Let $p(x) = 2x^7 - 7x^5 + 4x^3 - 9x + 1$ and let $q(x) = (x - 1)^4$.

- (a) Express each of the following elements of \overline{E} in the form $\overline{f(x)}$ for some polynomial $f(x)$ of degree ≤ 2 : $\overline{p(x)}$, $\overline{q(x)}$, $\overline{p(x) + q(x)}$, and $\overline{p(x)q(x)}$.
- (b) Prove that \overline{E} is not an integral domain.
- (c) Prove that \overline{x} is a unit in \overline{E} .

Proof. We proceed with each separately:

- (a) Do polynomial long division to figure out $\overline{p(x)}$ and $\overline{q(x)}$:

$$\begin{aligned} p(x) &= (2x^4 - 3x^2 - 2x - 2)(x^3 - 2x + 1) + (-x^2 - 11x + 3) \\ &\Rightarrow \overline{p(x)} = \overline{-x^2 - 11x + 3}; \\ q(x) &= (x - 4)(x^3 - 2x + 1) + (8x^2 - 13x + 5) \\ &\Rightarrow \overline{q(x)} = \overline{8x^2 - 13x + 5}. \end{aligned}$$

Then we have $\overline{p(x) + q(x)} = \overline{7x^2 - 24x + 8}$ and

$$\begin{aligned} \overline{p(x)q(x)} &= \overline{(-x^2 - 11x + 3)(8x^2 - 13x + 5)} \\ &= \overline{-8x^4 - 75x^3 + 162x^2 - 94x + 15} \\ \overline{p(x)q(x)} &= \overline{(-8x - 75)(x^3 - 2x + 1) + (146x^2 - 236x + 90)} \\ &\Rightarrow \overline{p(x)q(x)} = \overline{146x^2 - 236x + 90} \end{aligned}$$

- (b) Note that $x^3 - 2x + 1$ has a root at 1 so we may factor $x^3 - 2x + 1 = (x - 1)(x^2 + x - 1)$. However in the quotient, both $\overline{x - 1}$ and $\overline{x^2 + x - 1}$ are nonzero while $\overline{x^3 - 2x + 1} = \overline{0}$. Thus \overline{E} is not an integral domain.
- (c) We need $xf(x) = qd + 1$ where $d = x^3 - 2x + 1$ and q is some resulting quotient. Note that the LHS has no constant factor; hence a good guess for q would be -1 , since that eliminates the $+1$ on the RHS. Indeed, $\overline{xf(x)} = \overline{-d + 1} = \overline{-x^3 + 2x} = \overline{x(-x^2 + 2)}$. So clearly $\overline{f(x)} = \overline{-x^2 + 2}$ works. Then $\overline{f(x)} = \overline{-x^2 + 2}$ is the inverse of \overline{x} , proving that it is a unit.

□

Problem 30. Let I be an ideal of the commutative ring R and define

$$\text{rad } I = \{r \in R \mid r^n \in I \text{ for some } n \in \mathbb{Z}^+\}$$

called the *radical* of I . Prove that $\text{rad } I$ is an ideal containing I and that $(\text{rad } I)/I$ is the nilradical of the quotient ring R/I , i.e. $(\text{rad } I)/I = \mathfrak{N}(R/I)$.

Proof. $\text{rad } I$ contains I : Clearly for any $r \in I$ we have $r^1 \in I$, so $r \in \text{rad } I$. Thus $I \leq \text{rad } I$.

Recall that the nilradical of R/I is defined as

$$\{\bar{r} \in R/I \mid \bar{r}^n = 0 \text{ for some } n \in \mathbb{Z}^+\}.$$

Thus $\bar{r} \in \mathfrak{N}(R/I)$ if and only if there is $n \in \mathbb{Z}^+$ such that $\bar{r}^n = 0$. This occurs if and only if there is $n \in \mathbb{Z}^+$ such that $r^n \in I$, i.e. $r \in \text{rad } I$. Thus we may chain the if and only if statements to conclude that $(\text{rad } I)/I = \mathfrak{N}(R/I)$. □

Problem 31. An ideal I of the commutative ring R is called a *radical ideal* if $\text{rad } I = I$.

- (a) Prove that every prime ideal of R is a radical ideal.
- (b) Let $n > 1$ be an integer. Prove that 0 is a radical ideal in $\mathbb{Z}/n\mathbb{Z}$ if and only if n is a product of distinct primes to the first power (i.e. n is square free). Deduce that (n) is a radical ideal of \mathbb{Z} if and only if n is a product of distinct primes in \mathbb{Z} .

Proof. **TODO**

- (a) **TODO** Let P be a prime ideal of R . We already know that $P \leq \text{rad } P$, so it suffices to only show that $\text{rad } P \leq P$. Let $r \in \text{rad } P$ and $n \in \mathbb{Z}^+$ such that $r^n \in P$.

We proceed by induction to prove that $r^n \in P \Rightarrow r \in P$ for all $n \in \mathbb{Z}^+$. The base case $n = 1$ is trivial: $r \in P \Rightarrow r \in P$. Now assume for that sake of induction that

$r^k \in P \Rightarrow r \in P$ is true for some $k \in \mathbb{Z}^+$. Then consider $r^{k+1} = rr^k \in P$. Since P is prime, we have either $r \in P$, in which case we are done, or $r^k \in P$, in which case we may apply our IH to conclude that $r \in P$. This completes the induction.

Therefore we see that $r^n \in P \Rightarrow r \in P$, so $\text{rad } P \leq P$. Hence $\text{rad } P = P$ and P is a radical ideal.

(b) **TODO**

□

Exercises 1, 2, 5 pp. 267-269.

Problem 1. An element $e \in R$ is called an *idempotent* if $e^2 = e$. Assume that e is an idempotent in R and $er = re$ for all $r \in R$. Prove that Re and $R(1-e)$ are two-sided ideals of R and that $R \cong Re \times R(1-e)$. Show that e and $1-e$ are identities for the subrings Re and $R(1-e)$ respectively.

Proof. Re and $R(1-e)$ are two-sided ideals of R : Clearly Re is a two-sided ideal since $re = er \Rightarrow Re = eR$. Note that $(1-e)^2 = 1-2e+e^2 = 1-2e = e = 1-e$, so $1-e$ is an idempotent of R as well. Furthermore, for any $r \in R$ we have $r(1-e) = r - re = r - er - (1-e)r$, so $1-e$ commutes with everything. Clearly this shows that $R(1-e) = (1-e)R$; hence $R(1-e)$ is a two-sided ideal.

$R \cong Re \times R(1-e)$: Define the map $\varphi : R \rightarrow Re \times R(1-e)$ by $r \mapsto (re, r(1-e))$. Clearly φ is a surjective ring homomorphism, since both $r \mapsto re$ and $r \mapsto r(1-e)$ are surjective ring homomorphisms.

Thus it remains only to show that φ is injective. Indeed, suppose $\varphi(r) = (re, r(1-e)) = (0, 0)$. We have $re = 0$ and $r(1-e) = 0$; hence $r(1-e) = r - re = r = 0$, which shows that $\ker \varphi = 0$, as desired. We conclude that φ is an isomorphism and that

$$R \cong Re \times R(1-e).$$

View Re as a ring. Any element in Re has the form re for some $r \in R$. We can check that e is the identity directly: $(re)e = ree = re$ and $e(re) = e(er) = eer = er$. Similarly, view $R(1-e)$ as a ring. Since we've already shown that $1-e$ is an idempotent of R and $r(1-e) = (1-e)r$ for all $r \in R$, we have the same logic to show that $1-e$ is the identity: $r(1-e)(1-e) = r(1-e)$ and $(1-e)r(1-e) = r(1-e)(1-e) = r(1-e)$. □

Problem 2. Let R be a finite Boolean ring with identity $1 \neq 0$. Prove that $R \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \cdots \times \mathbb{Z}/2\mathbb{Z}$.

Proof. We proceed by induction on the cardinality of R . Consider the base case $|R| = 2$. Then there is only one choice for R , namely \mathbb{Z}_2 (we shorten $\mathbb{Z}/2\mathbb{Z}$), so our base case is correct.

Now assume for the sake of strong induction that our hypothesis holds for all $n < k$ for some $k > 2$. We want to show that any Boolean ring with size $|R| = n$ is isomorphic to some \mathbb{Z}_2^r .

Indeed, let $e \in R$ be any nonzero, non-identity element. Then $e^2 = e$ by definition, so e is an idempotent of R . We apply the previous exercise to give $R = Re \times R(1 - e)$. In particular, both Re and $R(1 - e)$ have at least two elements (zero and identity), so $|Re|, |R(1 - e)| < |R|$. Thus we may apply the induction hypothesis to see that

$$R \cong \mathbb{Z}_2^a \times \mathbb{Z}_2^b = \mathbb{Z}_2^{a+b}.$$

So we have $r = a + b$, and the induction is complete. \square

Problem 5. Let n_1, n_2, \dots, 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 $a_1, \dots, a_k \in \mathbb{Z}$ there is a solution $x \in \mathbb{Z}$ to the simultaneous congruences

$$x \equiv a_1 \pmod{n_1}, \quad x \equiv a_2 \pmod{n_2}, \quad \dots, \quad x \equiv a_k \pmod{n_k}$$

and that the solution x is unique mod $n = n_1 n_2 \dots n_k$.

- (b) Let $n'_i = n/n_i$ and t_i be the inverse of $n'_i \pmod{n_i}$. Prove that the solution x in (a) is given by

$$x = a_1 t_1 n'_1 + a_2 t_2 n'_2 + \dots + a_k t_k n'_k \pmod{n}.$$

- (c) Solve the simultaneous system of congruences

$$x \equiv 1 \pmod{8}, \quad x \equiv 2 \pmod{25}, \quad x \equiv 3 \pmod{81}$$

and

$$y \equiv 5 \pmod{8}, \quad y \equiv 12 \pmod{25}, \quad y \equiv 47 \pmod{81}.$$

Proof. **TODO** \square

More to be added...? **TODO**