

EXERCISES (page 255): Problems:

26. Let d be a positive integer. Prove that $\mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} | a, b \in \mathbb{Q}\}$ is a field.

Apply the "subring test" to $\mathbb{Q}[d] \subseteq \mathbb{R}$: (1'). $0 = 0 + 0\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$. Let $a + b\sqrt{d}, e + f\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$. Then, (1). $(a + b\sqrt{d}) - (e + f\sqrt{d}) = (a - e) + (b - f)\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$, since $a - e, b - f \in \mathbb{Q}$. (2). $(a + b\sqrt{d})(e + f\sqrt{d}) = ae + bdf + (af + be)\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$, since $ae + bdf, (af + be) \in \mathbb{Q}$. Since $\mathbb{Q}[\sqrt{d}] \subseteq \mathbb{R}$, $\mathbb{Q}[\sqrt{d}]$ is commutative and the multiplicative identity 1 of \mathbb{R} is in $\mathbb{Q}[\sqrt{d}]$ (since $1 = 1 + 0\sqrt{d}$). Let $a + b\sqrt{d} \neq 0 \in \mathbb{Q}[\sqrt{d}]$ (that is, not both a and b are zero). Then $(a + b\sqrt{d})^{-1} = \frac{1}{a + b\sqrt{d}} \frac{a - b\sqrt{d}}{a - b\sqrt{d}} = \frac{a}{a^2 - db^2} - \frac{b}{a^2 - db^2}\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$, since $\frac{a}{a^2 - db^2}, \frac{b}{a^2 - db^2} \in \mathbb{Q}$. So $\mathbb{Q}[\sqrt{d}]$ is a commutative ring with unity in which every non-zero element has an inverse.

38. Construct a multiplication table for $\mathbb{Z}_2[i]$, the ring of Gaussian integers modulo 2. Is this ring a field? Is it an integral domain?

	0	1	i	1+i
0	0	0	0	1+i
1	0	1	i	i
i	0	i	1	1+i
1+i	0	1+i	1+i	0

1+i is a zero divisor in $\mathbb{Z}_2[i]$. Hence $\mathbb{Z}_2[i]$ is not an integral domain. Therefore, $\mathbb{Z}_2[i]$ cannot be a field.

42. Suppose that a and b belong to a commutative ring and ab is a zero divisor. Show that either a or b is a zero-divisor. Since ab is a zero divisor of the ring (Note $ab \neq 0 \implies a \neq 0$ and $b \neq 0$), there exists $c \neq 0$ such that $(ab)c = 0$. Thus $a(bc) = 0$. Consider the following cases.

Case (1): Assume $bc=0$. Then b is a zero divisor since $b \neq 0$ and $c \neq 0$.

Case (2): Assume $bc \neq 0$. Then, from $a(bc) = 0$, a is a zero divisor since $a \neq 0$.

44. Suppose that R is a commutative ring without zero-divisors. Show that the characteristic of R is 0 or prime. If $\text{char } R = 0$, then we are done. Assume $\text{char } R = n > 0$. Suppose n is composite, say $n = n_1n_2$, $1 < n_1, n_2 < n$. $\exists a \neq 0 \in R$ such that $n_1a \neq 0$ and $\exists b \neq 0 \in R$ such that $n_2b \neq 0$. Then $(n_1a)(n_2b) = (n_1n_2)(ab) = n(ab) = 0$. So R has zero divisors n_1a and n_2a , a contradiction. Hence n must be a prime.

EXERCISES (page 269): Problems: 9. If n is an integer greater than 1, show that $\langle n \rangle = n\mathbb{Z}$ is a prime ideal of \mathbb{Z} if and only if n is prime.

Note $\langle n \rangle = n\mathbb{Z} = \{m \in \mathbb{Z} | n|m\}$.

(\implies) (\implies) Given: $\langle n \rangle = n\mathbb{Z}$ is a prime ideal of \mathbb{Z} Prove: n is prime.

Proof by Contradiction: Let n be composite. Then $n = rs$, $1 < r, s < n$. Now $r, s \in \{1, 2, \dots, n-1\}$ but the product $rs = n$ and $n|n$. So, $rs \in n\mathbb{Z}$. Since $n\mathbb{Z}$ is a prime ideal, either $r \in n\mathbb{Z}$ or $s \in n\mathbb{Z}$ (definition of a prime ideal). Thus, $n|r$ or $n|s$, a contradiction since $1 < r, s < n$ and neither r nor s are divisible by n .

(\impliedby) Given: n is prime.

Prove: $\langle n \rangle = n\mathbb{Z}$ is a prime ideal of \mathbb{Z} .

We know that $n\mathbb{Z}$ is a prime ideal of \mathbb{Z} . Let $a, b \in \mathbb{Z}$ such that $ab \in n\mathbb{Z}$. Then show that $a \in n\mathbb{Z}$ or $b \in n\mathbb{Z}$.

Now $ab \in n\mathbb{Z} \implies n|ab$ (definition of $n\mathbb{Z}$) $\implies n|a$ or $n|b$ (Euclid's Theorem, since n is prime) $\implies a \in n\mathbb{Z}$ or $b \in n\mathbb{Z}$ (definition of $n\mathbb{Z}$).

10. If A and B are ideals of a ring, show that the sum of A and B , $A + B = \{a + b \mid a \in A \text{ and } b \in B\}$, is an ideal. Apply the ideal test to $A + B$: (1'). $0 = 0 + 0 \in A + B$ (since $0 \in A$ and $0 \in B$). (1). Let $a + b, c + d \in A + B$. Then $(a + b) - (c + d) = (a - c) + (b - d) \in A + B$, since $a - c \in A$, and $b - d \in B$. (2). Let $r \in R$ and $a + b \in A + B$. Then $r(a + b) = ra + rb \in A + B$ (since $ra \in A$ and $rb \in B$) and $(a + b)r = ar + br \in A + B$ (since $ar \in A$ and $br \in B$).

14. Let A and B be ideals of a ring. Prove that $AB \subseteq A \cap B$.

Let $ab \in AB$. Then $ab \in A$ (since $a \in A$, b is in the ring, and A is an ideal) and $ab \in B$ (since $b \in B$, a is in the ring, and B is an ideal). Hence $ab \in A \cap B$ and $AB \subseteq A \cap B$.

1. What can be said about the characteristic of a ring $R \neq 0$ in which $x = -x \forall x \in R$? $x = -x \forall x \in R \implies 2x = 0 \forall x \in R \implies \text{char } R$ is positive and $\text{char } R \leq 2$. Thus $\text{char } R = 1$ or $\text{char } R = 2$. But $\text{char } R = 1 \implies 1x = 0 \forall x \in R \implies x = 0 \forall x \in R \implies R = \{0\}$, a contradiction since $R \neq 0$. Thus $\text{char } R = 2$.

2. Establish the following assertions concerning the characteristic of a ring R :

(a) if $\text{char } R > 0$, then $\text{char } S \leq \text{char } R$ for any subring S of R .

Assume $\text{char } R = n > 0$. Then $nr = 0 \forall r \in R \implies ns = 0 \forall s \in S$. Thus $\text{char } S > 0$ and $\text{char } S \leq n$. Hence $\text{char } S \leq \text{char } R$.

(b) if R is an integral domain and S is a subdomain of R , then $\text{char } S = \text{char } R$.

If 1 is the multiplicative identity (unity) of R , then $\text{char}(R)$ is equal to the additive order of 1 . Since S is a subdomain of R , it shares the unity 1 of R . So, $\text{char}(S)$ is equal to the additive order of 1 . Hence $\text{char}(S) = |1| = \text{char}(R)$.