Problem

Show that every ideal of $\mathbb{Z}$ is principal.

Proof: Let $n > 0$ be an integer. Suppose $I \subseteq \mathbb{Z}$ is an ideal. If $I = \{0\}$, then we are done since $I = (0)$, so suppose not. Since $\mathbb{Z} \neq \emptyset$, by the well-ordering principle, take n to be the smallest positive element in I.

$\boldsymbol{((n) \subseteq I)}$ Let $a \in (n)$. Then $a = nr$ for $r \in \mathbb{Z}$, and since $n \in I$, $nr \in I$. So $(n) \subseteq I$.

$\boldsymbol{((n) \supseteq I)}$ Let $a \in I$. Then $a = nq + r$ for unique $q, r \in \mathbb{Z}$. Note that since $a, n \in I$, we have $nq, r \in I$. We have that $r = 0$ since otherwise, $r < n$, which contradicts the assumption that n is the smallest element. This yields $a = nq \in (n)$, so $(n) \supseteq I$.

Therefore, $I = (n)$. Since n was arbitrary, every ideal of $\mathbb{Z}$ is principal.

Problem

Let $n > 0$ be an integer. Show that every ideal of $\mathbb{Z}/n$ is principal.

Proof: Let $n > 0$ be an integer and consider $\mathbb{Z}/n$. Define the canonical projection map $\pi : \mathbb{Z} \to \mathbb{Z}/n$ given by $a \mapsto [a]$. Let $I \subseteq \mathbb{Z}/n$, and let $J = \pi^{-1}(I) \subseteq \mathbb{Z}$ be the preimage of I under π. Since every ideal in $\mathbb{Z}$ is principal, write $J = (a)$ for some $a \in \mathbb{Z}$. We claim that $I = ([a])$.

$\boldsymbol{I \subseteq ([a])}$**:** Take $[x] \in I = \pi(\pi^{-1}(I)) = \pi(J)$. This implies that

$$x \in \pi^{-1}(\pi(J)) = \pi^{-1}(\pi((a))) = (a)$$

so $x = ar$ for some $r \in R$. Then $[x] = [ar] \in ([a])$, so $I \subseteq ([a])$.

$\boldsymbol{I \supseteq ([a])}$**:** Take $a \in J = (a)$. Since J is an ideal, we have that $ar \in J$ so we get

$$[ar] = [a][r] \in \pi(J) = \pi(\pi^{-1}(I)) = I$$

This implies that $([a]) \subseteq I$.

Therefore, $I = ([a])$ and every ideal in $\mathbb{Z}/n$ is principal.

Problem

Let $R = \mathbb{Z}/625$. Show that $([5])$ is a prime ideal. Is it maximal?

Proof: Let $R = \mathbb{Z}/625$. Consider $([5]) \subseteq \mathbb{Z}/625$. Define the canonical projection map $\mathbb{Z} \to \mathbb{Z}/625$ given by $a \mapsto [a]$. Note that $(625) \subseteq (5)$. Define $I = \pi((5)) = ([5])$. Then by the correspondence theorem, we have

$$R/I \cong \mathbb{Z}/(5)$$

Since 5 is prime, we have that (5) is prime. Further, since $\mathbb{Z}$ is a PID, we have that (5) is maximal, which shows that $\mathbb{Z}/(5)$ is a field. This implies that $I = \pi((5)) = ([5])$ is maximal and therefore also prime.

Problem

Suppose R is an integral domain. Show that prime elements are irreducible. If R is a PID, show that irreducibles are prime.

Proof: Let R be an integral domain and $p \in R$ be prime. Let $a \mid p$ for some $a \in R$. Then $ab = p$ for some $b \in R$ nonzero. Since p is prime, $p \mid ab$ so either $p \mid a$ or $p \mid b$. If $p \mid a$, then $a = px$ for some $x \in R$, so $ab = (px)b = p$. Since p is nonzero and R is an integral domain, apply the cancellation property to get $xb = 1$. This shows that b is a unit and implies that a is an associate of p. A similar argument can be made if $p \mid b$. Therefore, p is irreducible.

Let R be a PID and $p \in R$ be an irreducible. Consider $(p) \subseteq I = (a) \subseteq R$. Since $p \in (a)$, we have that $p = ab$ for $b \in R$. Since p is irreducible, either a or b is a unit. If a is a unit, then $(a) = R$. If b is a unit, then $(a) = (p)$. This implies that (p) is maximal, which further implies that (p) is prime. Since (p) is prime if and only if p is prime, we have that $p \in R$ is prime.

Problem

Suppose R is an integral domain. Show that maximal ideals are prime ideals. If R is a PID, show that prime ideals are maximal.

Proof: Let R be an integral domain. Let $M \subsetneq R$ be maximal. We want to show that M is prime; i.e. if $ab \in M$, then either $a \in M$ or $b \in M$. Let $ab \in M$. If $a \in M$, then we are done, so suppose not. Then $M + (a) = R$. Then $m + ar = 1$ for $m \in M$, $ar \in (a)$. Multiplying both sides by $b \in R$, we get $mb + arb = b$. But $ab \in M$ so $(ab)r \in M$. Therefore, we have $mb + abr = b \in M$. This shows that M is prime.

Let R be a PID. Let $P \subsetneq R$ be prime. We want to show that P is maximal; i.e. if there is an ideal $I \supsetneq P$, then $P + I = R$. Suppose we have $P \subsetneq I \subseteq R$. Since R is a PID, we have that $P = (p)$ and $I = (a)$ for $p, a \in R$. Then $p \in (p) \subsetneq (a)$, so $p = ar$ for $r \in R$. Since P is prime, either $a \in P$ or $r \in P$. If $a \in P$, then $(a) = (p)$. If $r \in P$, then $r = ps$ for some $s \in R$. Then we have $p = ar = a(ps) = p(as)$. Since R is an integral domain and p is nonzero, apply the cancellation property to get $1 = as$, which shows that a is a unit, so $(a) = R$. Therefore, P is maximal.

Problem

Suppose R is a commutative ring, let $I_1, I_2 \subseteq R$, and let $P \subseteq R$ be prime. Suppose $I_1 \cap I_2 \subseteq P$. Show that we either have $I_1 \subseteq P$ or $I_2 \subseteq P$.

Proof: Suppose R is a commutative ring, let $I_1, I_2 \subseteq R$, and let $P \subseteq R$ be prime. Suppose $I_1 \cap I_2 \subseteq P$. Suppose for the sake of contradiction that neither $I_1 \subseteq P$ nor $I_2 \subseteq P$. Take $a \in I_1 \setminus P$ and $b \in I_2 \setminus P$. Then $ab \in I_1$ and $ab \in I_2$ since they are both ideals. By definition, this means that $ab \in I_1 \cap I_2$. But $ab \in P$ and neither $a \in P$ nor $b \in P$, a contradiction.

Problem

Let R be an integral domain and $p \in R$. Show (p) is a prime ideal if and only if p is prime.

Proof: Let R be an integral domain and $p \in R$.

($\Longrightarrow$) Suppose (p) is a prime ideal. Consider $ab \in (p)$. Then by definition, $ab = pr$ for some $r \in R$, so $p \mid ab$. By definition of a prime ideal, either $a \in (p)$ or $b \in (p)$. Without loss of generality, suppose $a \in (p)$. Then $a = ps$ for some $s \in R$, so $p \mid a$. Therefore, p is prime.

($\Longleftarrow$) Suppose $p \in R$ is prime. Consider $p \mid ab$. Then either $p \mid a$ or $p \mid b$. Without loss of generality, suppose $p \mid a$. Consider the ideal generated by (p). Since $p \mid ab$, we have $ab = pr \in (p)$. Similarly, since $p \mid a$, we have $a = ps \in (p)$. Therefore, (p) is a prime ideal.

Since we have shown both directions, (p) is a prime ideal if and only if p is prime.

Problem

Let R be a commutative ring, and let $x \in R$ such that, for every maximal ideal $M \subseteq R$, we have $x \in M$. Show that $1 + x$ is a unit.

[Hint: You may use, without proof, the fact that any proper ideal is contained in a maximal ideal.]

Proof: Let R be a commutative ring, and let $x \in R$ such that, for every maximal ideal $M \subseteq R$, $x \in M$. Suppose for the sake of contradiction that $1 + x$ is not a unit. Consider the ideal generated by $1+x$. Then $(1+x) \subseteq M$, which implies that $1+x \in M$. But we also have $x \in M$, and since M is an ideal, it is closed under subtraction, so $1 + x - x = 1 \in M$. This is a contradiction.

Problem

Let R be a commutative ring, and let $S \subseteq R$ be the *subset* of nonunits. Show that the following are equivalent:

(a) The set S forms a maximal ideal of R.

(b) R has a unique maximal ideal.

[Hint: You may use, without proof, the fact that any proper ideal is contained in a maximal ideal.]

Proof: Let R be a commutative ring, and let $S \subseteq R$ be the *subset* of nonunits.

(a) $\implies$ (b): Suppose the set S forms a maximal ideal of R. Then suppose for the sake of contradiction that there exists another maximal ideal $M \subsetneq R$. Take $x \in M \setminus S$. This implies that x is a unit since S is the subset of nonunits, a contradiction. Therefore, S is the unique maximal in R.

(a) $\impliedby$ (b): Suppose R has a unique maximal M. We claim that $M = S$. Clearly, $M \subseteq S$ since otherwise, M contains at least one unit, a contradiction. Consider the ideal generated by $x \in S$. Since x is not a unit, $(x) \subsetneq R$, so $(x) \subseteq M$. Therefore, $M = S$, which shows that S is maximal.

Problem

Let $f : R \to S$ be surjective, and let $P \subseteq S$ be a prime ideal. Show that $f^{-1}(P) \subseteq R$ is a prime ideal.

Proof: Suppose $f : R \to S$ is a surjective ring homomorphism and $P \subseteq S$ is prime. Consider the ideal $f^{-1}(P) \subseteq R$. Take $a, b \in R$ such that $ab \in f^{-1}(P)$. Then $f(ab) = f(a)f(b) \in P$. Since P is prime, either $f(a) \in P$ or $f(b) \in P$. Then by definition of the preimage, either $f^{-1}(f(a)) = a \in f^{-1}(P)$ or $f^{-1}(f(b)) = b \in f^{-1}(P)$, which shows that $f^{-1}(P)$ is prime.

Problem

Let $f : R \to S$ be surjective, and let $M \subseteq S$ be a maximal ideal. Show that $f^{-1}(M) \subseteq R$ is a maximal ideal.

Proof: Suppose $f : R \to S$ is a surjective ring homomorphism and $M \subseteq S$ is maximal. Consider the ideal $f^{-1}(M) \subseteq R$. Let $N \supseteq f^{-1}(M)$. Then $f(N)$ is an ideal since

(1) N is an ideal so $0 \in N$. Then $f(0_R) = 0_S \in f(N)$.

(2) Take $c, d \in f(N)$. Then sine f is surjective, there exist, $a, b \in N \subseteq R$ such that $f(a) = c, f(b) = d$. Then since N is an ideal, it is closed under subtraction so $a - b \in N$ which implies that $f(a - b) = f(a) - f(b) = c - d \in f(N)$.

(3) Take $c \in f(N)$, $s \in S$. Since f is surjective, there exist $a \in N, r \in R$ such that $f(a) = c, f(r) = s$. Then since N is an ideal, $ar \in N$ so $f(ar) = f(a)f(r) = cs \in f(N)$.

Now we claim that $f(f^{-1}(M)) = M$. To see $f(f^{-1}(M)) \subseteq M$, take $f(x) \in f(f^{-1}(M))$. Then by definition of the preimage, $x \in f^{-1}(M)$ which implies that $f(x) \in M$. To see $f(f^{-1}(M)) \supseteq M$, take $y \in M$. Since f is surjective, there exists $x \in R$ such that $f(x) = y \in M$. This implies that $x \in f^{-1}(M)$, so $f(x) \in f(f^{-1}(M))$. Thus, $f(f^{-1}(M)) = M$.

Since M is maximal, either $f(N) = S$ or $f(N) = M$. If $f(N) = S$, then since f is surjective, N maps onto all of S, which is only true when $N = R$. If $f(N) = M$, then $N = f^{-1}(M)$. Therefore, $f^{-1}(M)$ is maximal.

Problem

Let R be an integral domain. Suppose $R[x]$ is a principal ideal domain. Show that R must be a field.
[Hint: Think about (x).]

Proof: Let R be an integral domain and $R[x]$ a principal ideal domain. Consider the principal ideal $(x) \subseteq R[x]$ and a function $f : R[x] \to R$ with $f(p(x)) = p(0)$. Then

- $f(p(x) + q(x)) = p(0) + q(0) = f(p(x)) + f(q(x))$, so f is **closed under addition**.
- $f(p(x) \cdot q(x)) = p(0) \cdot q(0) = f(p(x)) \cdot f(q(x))$, so f is **closed under multiplication**.
- $f(1(x)) = 1$, so f **preserves the multiplicative identity**.

so f is a ring homomorphism. We have that $\ker(f) = \{p(x) : f(p(x)) = 0\} = (x)$, so $\ker(f) = (x)$. To show $\mathrm{Im}(f) = R$, take $a \in R$. Then consider $p \in R$ such that $p(0) = a$. Then $f(p(x)) = p(0) = a \in R$. Therefore, $\mathrm{Im}(f) = R$. Then by the **First Isomorphism Theorem**, we have that $R[x]/(x) \simeq R$.

To show (x) is maximal, we will show that x is irreducible. Consider $x = ab$. Then $\deg(x) = \deg(a) + \deg(b)$. Without loss of generality, suppose $\deg(a) = 0$. Then $b = cx + d$ for $c, d \in R$, so we have $x = ab = a(cx + d) = acx + ad$, but $x + 0 = acx + ad$ which implies that $ad = 0$, so $x = acx$. Since $R[x]$ is an integral domain, apply the cancellation property to get $1 = ac$. This shows that a is a unit. Therefore, x is irreducible. Since $R[x]$ is a PID, irreducibles are prime, so (x) is a prime ideal. Further, since $R[x]$ is a PID, prime ideals are maximal, so (x) is maximal. This shows that $R[x]/(x)$ is a field, which is isomorphic to R, so R is a field.