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.

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

($(n) \supseteq I$) 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 $(n) \subseteq \mathbb{Z}$. Since every ideal in $\mathbb{Z}$ is principal, (n) is a principal ideal. Then consider $\mathbb{Z}/(n)$ and $J \subseteq \mathbb{Z}/(n)$. Define the canonical projection $\pi : \mathbb{Z} \to \mathbb{Z}/(n)$ given by $a \mapsto [a]$. Then the preimage of J under π is given by $\pi^{-1}(J) \supseteq (n)$. Since $\pi^{-1}(J) \subseteq \mathbb{Z}$, it is principal, so we have $\pi^{-1}(J) = (a)$ for some $a \in \mathbb{Z}$. Then by the correspondence theorem, we have

$$\begin{aligned}
\pi(\pi^{-1}(J)) &= \pi((a)) \\
&= \{\pi(ar) : r \in \mathbb{Z}\} \\
&= \{[ar] : r \in \mathbb{Z}\} \\
&= \{[a][r] : [r] \in \mathbb{Z}/n\} \\
\pi(\pi^{-1}(J)) &= ([a])
\end{aligned}$$

But $\pi(\pi^{-1}(J)) = J$, so $J = ([a])$. This shows that $J \subseteq \mathbb{Z}/(n)$ is principal. Since J was arbitrary, 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 $([5])$.

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 $p \in R$.

($\implies$) 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.

($\impliedby$) 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.