Recall:

Def: A *ring* R is an Abelian group under addition, with an additional binary operation multiplication such that multiplication is associative and multiplication is distributive over addition.

Definition: A **field** is a commutative ring with unity in which every non-zero element is a unit.

Def: Definition: A **zero-divisor** is a non-zero element a of a commutative ring R such that there is a non-zero element $b \in R$ with $ab = 0$.

Questions:

1. We know that rings that have the cancellation property $a \neq 0$ and $ab = ac \Rightarrow b = c$ can not have zero-divisors. Is *not* having zero divisors enough to give a ring the cancellation property?
2. Can fields have zero-divisors?
3. Is *not* having zero-divisors enough to make a commutative ring with unity a field?

In Class Work

1. Show that every nonzero element of $\mathbb{Z}_n$ is either a unit or a zero-divisor.
2. Find an element in $\mathbb{Z}[x]$ which is neither a unit nor a zero-divisor.
3. Suppose that a and b belong to an integral domain.
   3.1 If $a^5 = b^5$ and $a^3 = b^3$, prove that $a = b$.
   3.2 If $a^m = b^m$ and $a^n = b^n$, where m and n are relatively prime integers, prove that $a = b$.
4. Let R be a ring with unity. If the product of any pair of nonzero elements of R is nonzero, prove that $ab = 1$ implies that $ba = 1$.

Solutions

1. Show that every nonzero element of $\mathbb{Z}_n$ is either a unit or a zero-divisor.
Let $a \neq 0 \in \mathbb{Z}_n$ such that a is not a unit. NTS a is a zero divisor. In other words, NTS $\exists\ b \neq 0$ such that $ab = 0$ in $\mathbb{Z}_n$.
Remember from Friday, the units of $\mathbb{Z}_n$ are those elements relatively prime to n, or $U(n)$.
Thus if a is not a unit, $gcd(a, n) = k \neq 1$.
Let $b = \frac{n}{k}$. $b \in \mathbb{Z}$, and $0 < b < n$ so $b \in \mathbb{Z}_n$.

$$ab = a\left(\frac{n}{k}\right) = \left(\frac{a}{k}\right)n.$$

Since $k|a$,

$$ab = cn = 0 \mod n.$$

Thus a is a zero divisor in $\mathbb{Z}_n$.

3. Suppose that a and b belong to an integral domain.

1. If $a^5 = b^5$ and $a^3 = b^3$, prove that $a = b$.

$$a^3 = b^3 \Rightarrow a^6 = b^6 \Rightarrow a^5 a = b^5 b \Rightarrow a^5 a = a^5 b$$

   Since in a domain, we have cancellation, $a = b$

2. If $a^m = b^m$ and $a^n = b^n$, where m and n are relatively prime integers, prove that $a = b$.
   Because $\gcd(m, n) = 1$, $\exists\ s, t$ such that $sm + tn = 1$.

4. Let R be a ring with unity. If the product of any pair of nonzero elements of R is nonzero, prove that $ab = 1$ implies that $ba = 1$.
Assume a, b are elements such that $ab = 1$. Need to show that $ba = 1$ as well. (In other words, that the left and right inverses are the same, *in this case*).
Note that $ab = 1$ means that neither $a = 0$ nor $b = 0$.

$$ab = 1 \Rightarrow (ab)a = a \Rightarrow a(ba) - a = 0 \Rightarrow a(ba - 1) = 0$$

Since the product of any pair of nonzero elements is nonzero and since $a \neq 0$, $ba - 1$ must be 0.
Thus $ba = 1$.