Exercises
Math 225 Modern Algebra
Fall 2017

42. Several properties of divisibility follow directly from the definition just like they do with the integral domain is $\mathbf{Z}$. Prove the following properties from the above definitions.

(a). 1 divides every element.
(b). Each element divides itself.
(c). If $a \mid b$ then $a \mid bc$.
(d). Divisibility is transitive.
(e). If one element divides two other elements, then it divides both their sum and difference.
(f). Cancellation: When $c \neq 0$, $a \mid b$ if and only if $ac \mid bc$.

(a). By the definition, $1 \mid b$ means there is some c such that $1c = b$. There is such a c, namely, $c = b$. Thus 1 divides every element. Q.E.D.

(b). $b \mid b$ means there is some c such that $bc = b$. There is such a c, namely, $c = 1$. Thus each element divides itself. Q.E.D.

(c). Suppose that $a \mid b$. Then there is a d such that $ad = b$. Therefore $a(dc) = bc$, so $a \mid bc$. Thus $a \mid b$ implies $a \mid bc$. Q.E.D.

(d). Suppose that $a \mid b$ and $b \mid c$. Then there exists a d such that $ad = b$, and there exists an e such that $be = c$. Therefore $a(de) = be = c$, so $a \mid c$. Thus divisibility is transitive. Q.E.D.

(e). Suppose that $a \mid b$ and $a \mid c$. Then there exists a d such that $ad = b$, and there exists an e such that $ae = c$. Therefore $a(d+e) = b+c$ and $a(d-e) = b-c$, so $a \mid (b+c)$ and $a \mid (b-c)$. Thus, iff one element divides two other elements, then it divides both their sum and difference. Q.E.D.

(f). Let c be a nonzero element in an integral domain.

First, suppose that $a \mid b$. Then $ad = b$ for some d, so $(ac)d = bc$, so $ac \mid bc$.

Next, suppose that $ac \mid bc$. Then $acd = bc$ for some d. In an integral domain we can cancel the c's since c is not zero to conclude $ad = b$, so $a \mid b$. Q.E.D.

43. Prove that a nonzero element x is an integral domain D is prime if and only if the principal ideal (x) is a prime ideal.

Recall what the two statements mean.

A nonzero element x is prime when it's not a unit and whenever $x \mid yz$, either $x \mid y$ or $x \mid z$.

The ideal (x) is a prime ideal when (1) $(x) \neq D$, and (2) for all $y, z \in D$, if $yz \in (x)$, then either $y \in (x)$ or $z \in (x)$.

Proof.
$\Rightarrow$: Suppose that x is prime. Then it's not a unit so $(x) \neq (1)$ which means $(x) \neq D$. Now let $yz \in (x)$. Then $x \mid yz$. Therefore $x \mid y$ or $x \mid z$. If $x \mid y$ then $y \in (x)$, but if $x \mid z$ then $z \in (x)$. Thus either $y \in (x)$ or $z \in (x)$. Thus (x) is a prime ideal.

$\Leftarrow$: Suppose that (x) is a prime ideal. Since $(x) \neq D$, therefore x is not a unit. Now let $x \mid yz$. Then $yz \in (x)$. Therefore either $y \in (x)$ or $z \in (x)$. In the first case $x \mid y$, and in the second case $x \mid z$. So either $x \mid y$ or $x \mid z$. Thus x is prime. Q.E.D.

Math 225 Home Page at
`http://aleph0.clarku.edu/~djoyce/ma225/`