Abstract Algebra I - Lecture 10

Adam Chapman

Department of Mathematics, Michigan State University, East Lansing, MI 48824

---

Divisibility and congruence in rings.
Let $R$ be commutative a ring and let $a, b \in R$. We say that $a$ divides $b$ and write $a \mid b$ if there exists $c \in R$ such that $a \cdot c = b$. $b$ is then called a multiple of $a$ and $a$ is a divisor of $b$.

Examples.

- In $\mathbb{Z}$, $2 \mid 4$ and $2 \not\mid 3$.
- In $\mathbb{Q}$, $2 \mid 4$ and $2 \mid 3$ because $2 \cdot \frac{3}{2} = 3$.
- In $2\mathbb{Z}$, $2 \not\mid 6$.
- Given a ring $R$, $x \mid f(x)$ in $R[x]$ if and only if the free coefficient of $f(x)$ is zero.
- $2x \mid x^2$ in $\mathbb{Q}[x]$ but $2x \not\mid x^2$ in $\mathbb{Z}[x]$.

Remark.
Given a ring $R$, $r \mid 0$ for any $r \in R$. If $0 \mid r$ then $r = 0$. If $R$ has an identity then $r \mid r$ for any $r \in R$.

Proof.
For any $r \in R$, $r \cdot 0 = 0$, so $r \mid 0$.
Assume $0 \mid r$. This means that $0 \cdot x = r$ for some $x \in R$. However, $0 \cdot x = 0$, which means that $0 = r$.
If $R$ has an identity $1$ then $r \cdot 1 = r$ and so $r \mid r$.

Remark.
1. If \(a|b\) and \(b|c\) then \(a|c\).
2. If \(a|b\) then \(-a|b\) and \(a| -b\).
3. If \(a|b\) and \(a|c\) then \(a|(b + c)\) and \(a|bc\).

**Proof.**

1. \(b = a \cdot r\) and \(c = b \cdot s\), so \(c = (a \cdot r) \cdot s = a \cdot (r \cdot s)\), so \(a|c\).
2. If \(b = a \cdot r\) then \(-b = -(a \cdot r) = a \cdot (-r)\). Furthermore \(b = -(-b) = -(a \cdot (-r)) = (-a) \cdot (-r)\).
3. If \(b = a \cdot r\) and \(c = a \cdot s\) then \(b + c = a \cdot r + a \cdot s = a \cdot (r + s)\) and \(bc = (a \cdot r) \cdot (a \cdot s) = a \cdot (a \cdot r \cdot s)\).

**Question.**
If \(a|b\) and \(c|b\), does it mean \((a + c)|b\)? Does it mean \(ac|b\)?

**Answer.**
No and no. Consider the ring \(\mathbb{Z}\) and take \(a = b = c = 2\). Then \(a|b\) and \(c|b\) but \(a + c \not|b\) and \(ac \not|b\).

**Congruence.**

Given a ring \(R\) and an element \(n\), one can define an equivalence relation \(a \equiv b \pmod{n}\) by \(n|a - b\). [Show that this is indeed an equivalence relation as a home exercise.] Then one can discuss the corresponding equivalence class of \(a\), \([a] = \{b \in R : a \equiv b \pmod{n}\}\), and the set of equivalence classes is denoted by \(R_n\) or \(R/\equiv \pmod{n}\).

**Examples.**

- Any \(n \in \mathbb{Z}\) gives rise in this way to \(\mathbb{Z}_n\). Note that \(\mathbb{Z}_0\) by this definition is infinite, because every two different integers \(a\) and \(b\) are not equivalent modulo 0 (0 divides only itself). Note also that \(\mathbb{Z}_1\) contains only one congruence class, the set \(\mathbb{Z} = [0]_1\).

- Take \(R = \mathbb{R}[x]\). Then \(R_n\) is \([r] : r \in \mathbb{R}\). For example, \(1 + x \equiv 1 + x^2 \pmod{x}\). To be more precise, every polynomial \(f(x) = c_0 + c_1x + \cdots + c_nx^n\) can be written as \(f(x) = c_0 + x(c_1 + \cdots + c_nx^{n-1})\) and so \(f(x) \equiv c_0 \pmod{x}\). Of course, \(x\) does not divide any nonzero real number, so free coefficient determines uniquely the congruence class of the polynomial.

- Take \(R = \mathbb{Z}_6\). Then \(R_{[3]}\) is \([[[0]], [[1]], [[2]]]\). Notice that \([[0]] = \{[0], [3]\}, [[1]] = \{[1], [4]\}\) and \([[2]] = \{[2], [5]\}\).
Exercise.
In a commutative ring \( R \) with identity, prove that if \( a \) is a zero divisor and \( b \) is a unit then \( a \not| b \). Give an example where \( b|a \).
Consider \( R = \mathbb{Z}[x] \). Say whether the following congruences if they hold:

- \( x^2 + 4x^5 \equiv 6 - x^2 + 2x^3 + 4x^5 \pmod{2} \).
- \( x^2 + 4x^5 \equiv 6 - x^2 + 2x^3 + 4x^5 \pmod{x} \).
- \( x^2 + 4x^5 \equiv 6 - x^2 + 2x^3 + 4x^5 \pmod{3} \).
- \( x^2 + 4x^5 \equiv 6 - x^2 + 2x^3 + 4x^5 \pmod{4} \).

Let \( m, n \in \mathbb{Z} \). What is \( m\mathbb{Z} \cap n\mathbb{Z} \)? Say whether the following statements hold:

- \( 12 \in 4\mathbb{Z} \cap 6\mathbb{Z} \).
- \( 6 \in 4\mathbb{Z} \cap 6\mathbb{Z} \).
- \( 24 \in 4\mathbb{Z} \cap 6\mathbb{Z} \).