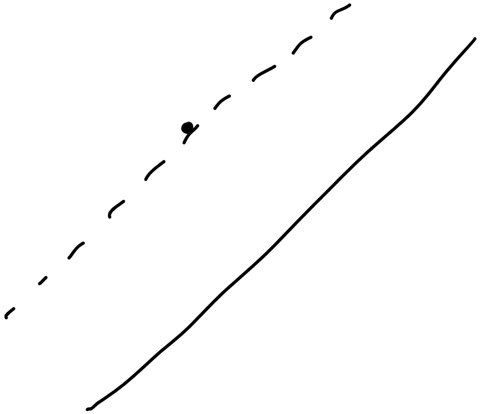
Chapter 4 section 1-2 cont'd

Chapter 4 section 1-2 cont'd

Axioms

Our book does not mention axioms but it should. Axioms are statements that are asserted to be true for purposes of constructing a theory. For example:

Axiom: Given a line L, and a point P not on L, there is exactly one line through P parallel to L.



Axiom: An empty set exists.

Axioms in this course

- Existence of integers, natural numbers, rational numbers, and real numbers.
- Properties of addition, multiplication such as commutative and associative laws, including closure.
- Properties of $>$ and $<$

2 natural numbers do arithmetic → natural number.

Let X be $\mathbb{R}, \mathbb{Q}, \mathbb{Z}$ or $\mathbb{N}$.

Given any two elements $a, b \in X$ ($\forall a, \forall b$ $a, b \in X$)

we have $a+b \in X$
$ab \in X$.

$\mathbb{N}$ $\mathbb{R}$ $\mathbb{Q}$ $\mathbb{Z}$

sums products of rat'l numbers are rational

integers

The Division Algorithm

$\forall a, b \in \mathbb{Z}$ with $b > 0$

The Division Algorithm: Given $a, b \in \mathbb{Z}$ with $b > 0$, there are unique integers q and r with $0 \leq r < b$ so that $a = bq + r$.

$a = 41 \qquad b = 7$

$q \qquad r \qquad 0 \leq r < 7$

$41 = 7q + r$

$41 = 5 \cdot 7 + 6$

$$\begin{array}{r} 5 \\ 7 \overline{)41} \\ 35 \\ \hline 6 \end{array}$$

$41 - 5 \cdot 7 = 6$

$$\begin{array}{r} 41 \\ -7 \\ \hline 34 \\ -7 \\ \hline 27 \\ -7 \\ \hline 20 \\ -7 \\ \hline 13 \end{array} \qquad \begin{array}{r} -7 \\ \hline 6 \end{array}$$

$-33 = \cancel{b}\, 7q + r$

$-33 + 5 \cdot 7 = 2$

$-33 = (-5)7 + 2$

The Fundamental Theorem of Arithmetic

Theorem: Every natural number greater than one is a product of prime numbers, and this factorization into primes is unique up to rearranging the terms.

$$33 = 3 \cdot 11$$

$$72 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3$$

$$112 = 2 \cdot 56 = 2 \cdot 2 \cdot 28 = 2 \cdot 2 \cdot 2 \cdot 14$$

$$= 2 \cdot 2 \cdot 2 \cdot 2 \cdot 7$$

Some fundamental definitions: divisibility

Definition: Suppose a and b are integers. We say that a **divides** b, written $a|b$, if $b = ac$ for some $c \in \mathbb{Z}$. In this case we also say that a is a divisor of b and that b is a multiple of a.

$a|b$ $\quad a/b \quad a\backslash b$

$a|b$ means: there exists $c \in \mathbb{Z}$ so that $b = ac$

$14|28$ means: there exists $c \in \mathbb{Z}$ so that $28 = 14c$

true because $c = 2$ works.

$a|b \iff$ a is a divisor of b $\iff$ b is a multiple of a

GCD and LCM

Definition: The greatest common divisor of integers a and b, written $\gcd(a, b)$, is the largest integer that divides both a and b.

Definition: The least common multiple of integers a and b, written $\operatorname{lcm}(a, b)$, is the smallest integer that is a multiple of both a and b.

$\gcd(8,12)$ = largest integer d such that $d \mid 8$ and $d \mid 12$.

1, 2, 4, 8 are divisors of 8

1, 2, 3, 4, 6, 12 " " " 12

$\operatorname{lcm}(8,12)$ = smallest integer d so that $8 \mid d$ and $12 \mid d$

$\operatorname{lcm}(8,12) = 24$

multiples of 8: 8, 16, 24, 32, 40, 48, 56, ...

multiples of 12: 12, 24, 36, 48, ...