Selected Answers for Contemporary Abstract Algebra

Ian Shaw

July 28, 2020

These are write-ups for the questions left to the reader in Joseph A. Gallian's 8th edition of *Contemporary Abstract Algebra*. The questions were selected because they were the most interesting.

Contents

1 Chapter 0: Preliminaries

5. Show that if a and b are positive integers, then $ab = \operatorname{lcm}(a,b) \bullet \gcd(a,b)$.

Proof. By the Fundamental Theorem of Arithmetic (Theorem 0.3 in the book) that a is the product of primes, and by definition the greatest common divisor is a product of a subset of these primes

$$a = \gcd(a,b)\prod_{i=1}^{n} p_{a,i}$$

Since by this definition

$$\{\emptyset\} = \{p_{a,i}\} \cap \{p_{b,i}\}$$

Thus

$$\operatorname{lcm}(a,b) = \gcd(a,b)\prod_{i=1}^{n} p_{a,i}\prod_{j=1}^{m} p_{b,j}$$

Therefore

$$\begin{aligned}
\operatorname{lcm}(a,b)\gcd(a,b) &= \gcd(a,b)\gcd(a,b)\prod_{i=1}^{n} p_{a,i}\prod_{j=1}^{m} p_{b,j} && (1)\\
&= \big(\gcd(a,b)\prod_{i=1}^{n} p_{a,i}\big)\big(\gcd(a,b)\prod_{j=1}^{m} p_{b,j}\big) && (2)\\
&= ab && (3)
\end{aligned}$$

□

7. If a and b are integers and n is a positive integer, prove that $a \bmod n = b \bmod n$ if and only if n divides $a - b$.

Proof. Forward: If $a \bmod n = b \bmod n$, then n divides $a - b$. So we know that

$$\begin{aligned} m_a, m_b, r, &\in \mathbb{Z} && (4)\\ a &= m_a n + r && (5)\\ b &= m_b n + r && (6)\\ & && (7) \end{aligned}$$

Doing some artihmetic

$$a - b = (m_a - m_b)n \implies n|(a - b)$$

Backward: If n divides $a - b$, then $a \bmod n = b \bmod n$.

$$\begin{aligned} mn &= a - b && (8)\\ a &= mn + b && (9) \end{aligned}$$

We also know by the Division Algortihm

$$\begin{aligned} b &= m_b n + r\\ r &= b \bmod n \end{aligned}$$

Thus with substitution

$$\begin{aligned} a &= mn + m_b n + r && (10)\\ &= n * (m - m_b) + r \implies r = a \bmod n && (11) \end{aligned}$$

□

2 Notation

Throughout the paper, we will reference the notation listed in this section.

$$\begin{aligned} \mathbb{Z} &= \text{integers} && (12)\\ \mathbb{Z}^+ &= \text{positive integers} && (13)\\ & && (14) \end{aligned}$$