

Homomorphism of groups

Remember that an isomorphism from a group $[G_1, *_1]$ to a group $[G_2, *_2]$ is a bijection f from G_1 satisfying the relation

$$(*) \quad f(a *_1 b) = f(a) *_2 f(b) \text{ for all } a, b \text{ in } G_1.$$

If we *drop* the requirement that f be bijective, then what we have is the notion of a *homomorphism*. For instance, there is no bijection from \mathbb{Z} to \mathbb{Z}_2 , so there certainly isn't an isomorphism, but there is a map f from \mathbb{Z} to \mathbb{Z}_2 that sends the even integers to 0 and the odd integers to 1, and it has property (*).

You can check that $f(a + b) = a +_2 b$ for all integers a, b . This means that if you want to know the remainder when you divide $a + b$ by 2, compute the remainder r that you get when you divide a by 2 and the remainder s that you get when you divide b by 2 and then compute $r +_2 s$.

Note that if f is a homomorphism, then the formula $f(a *_1 b) = f(a) *_2 f(b)$ extends automatically to bigger formulas like $f(a *_1 b *_1 c) = f(a) *_2 f(b) *_2 f(c)$.

There is a homomorphism from \mathbb{Z} to \mathbb{Z}_{10} that maps 17 to 7, 1023 to 3, -14 to 6, and more generally maps each nonnegative integer to its last digit (and maps each negative integer to 9 minus its last digit). That is, this homomorphism sends every n to $n \% 10$. The homomorphism property is related to the fact that if you know the last digit of the positive integer a and the last digit of the positive integer b , then you can deduce the last digit of the positive integer $a + b$.

A historically important homomorphism is the function f from \mathbb{Z} to \mathbb{Z}_9 that sends every n to $n \% 9$. It is easy to compute $n \% 9$ for any positive integer n : just add the digits of n , obtaining a new number n' , and then add the digits of n' , obtaining a new number n'' , and so on, until you arrive at a single-digit number s ; if s is 9, then $n \% 9 = 0$, otherwise $n \% 9 = s$. For instance, with $n = 1234567$, we get $n' = 1 + 2 + 3 + 4 + 5 + 6 + 7 = 28$ and $n'' = 2 + 8 = 10$ and $n''' = 1 + 0 = 1$, so $f(n) = n \% 9 = 1$. This homomorphism is at the heart of the method of casting out nines, one of the earliest attempts at error-checking. The idea is that if you added two big integers a and b and got c , then $f(c)$ should be $f(a) +_9 f(b)$ in \mathbb{Z}_9 . Turning this around, if $f(a) +_9 f(b)$ isn't $f(c)$, then we must have made a mistake when we computed c . This method doesn't tell you where you made the mistake – only that you made one. But for many purposes that's the right first step.

I'll conclude with two examples of homomorphisms related to Exercise 11.7.8(a) from the textbook. The operation $\text{abs}(\cdot)$ from $[\mathbb{R}^*, \times]$ to $[\mathbb{R}^+, \times]$ that sends x to $|x|$ is a homomorphism because $\text{abs}(x \times y) = \text{abs}(x) \times \text{abs}(y)$ (that is, $|xy| = |x||y|$) for all nonzero x, y . Likewise, the operation $\text{sign}(\cdot)$ from $[\mathbb{R}^*, \times]$ to $[\{1, -1\}, \times]$ that sends x to $+1$ if x is positive and -1 if x is negative is a homomorphism because $\text{sign}(xy) = \text{sign}(x)\text{sign}(y)$ for all nonzero x, y .