MATH 351 – Modern Algebra 1
Selected Solutions for Problem Set 6
October 27, 2018

4.32

1. $\mathbb{Z}_9 \times \mathbb{Z}_3$ is *not isomorphic to* $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$. The fastest way to get to this conclusion is to notice that $(1, 0)$ is an element of order 9 in the first group, but there are no elements of order 9 in the second. In fact every $(a, b, c) \in \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ has order either 1 or 3. Therefore, Theorem 4.17 part 4 shows that the groups are not isomorphic.

2. $\mathbb{Z}_{21} = \langle 1 \rangle$ is a cyclic group under addition because the order $|1| = 21$. On the other hand, the element $(1, 1) \in \mathbb{Z}_3 \times \mathbb{Z}_7$ also has order 21, as you can check easily: the first time you get $(0, 0)$ for positive multiples of $(1, 1)$ is $21 \cdot (1, 1)$, since $\gcd(3, 7) = 1$ implies $\mathrm{lcm}(3, 7) = 1$. Since both groups are cyclic of order 21, Theorem 4.14 implies *they have to be isomorphic.*

3. This is similar to 2. Both $U(22)$ and $\mathbb{Z}_{10}$ are cyclic groups of order 10. You can check for instance that $U(22) = \langle 7 \rangle$ since in $U(22)$

$$7^1 = 7, 7^2 = 5, 7^3 = 13, 7^4 = 3, 7^5 = 21, 7^6 = 15, 7^7 = 17, 7^8 = 9, 7^9 = 19, 7^{10} = 1$$

   So *they are isomorphic* by Theorem 4.14.

4. These groups are *not isomorphic* because $\mathbb{Z}_2 \times \mathbb{Z}_{10}$ is abelian, but D_{20} is not. (Recall from class on Friday, October 26, in D_{20}, we would have the relation $FR_{360/10} = (R_{360/10})^{-1}F$, where F is one of the flips.

   4.40. A large proportion of this problem is just thinking up a mapping from $\mathbb{Q}^+$ (the group of positive rationals under multiplication) and the group H:

$$H = \{(a_1, a_2, a_3, \dots) \mid a_i \in \mathbb{Z}, \text{ and there exists } k_0 \text{ such that } a_k = 0 \text{ for all } k \geq k_0\}.$$

   Here's a suitable mapping $\alpha : \mathbb{Q}^+ \to H$. Recall that we can factor the numerator and denominator in an integer fraction m/n into products of prime numbers in $\mathbb{Z}$. Only finitely many primes appear with nonzero exponents, so if we make the vector of exponents (say, taking the primes in increasing order, and listing the exponents in the same order), then we get an element of H from each $m/n \in \mathbb{Q}^+$:

$$\begin{aligned} \alpha : \mathbb{Q}^+ &\longrightarrow H \\ 2^{a_1} 3^{a_2} 5^{a_3} \cdots &\longmapsto (a_1, a_2, a_3, \dots) \end{aligned}$$

   This is well-defined by the uniqueness of prime factorizations, and we will agree to combine the exponents in the case that m/n is not in lowest terms (written as a reduced fraction with $\gcd(m,n) = 1$). Note that negative a_i would correspond to primes dividing the denominator. For instance, $45/49 = 3^2 \cdot 5 \cdot 7^{-2}$, so we would get

$$\alpha\left(\frac{45}{49}\right) = (0, 2, 1, -2, 0, 0, \dots);$$

because no prime greater than 7 divides the top or the bottom, the components of $\alpha(45/49)$ for all primes ≥ 11 are zero.

Now we claim that α is an isomorphism of groups.

- It is a group homomorphism because of the usual rules for exponents (in $\mathbb{Q}^+$): If $m/n = 2^{a_1}3^{a_2}5^{a_3}\cdots$ and $m'/n' = 2^{b_1}3^{b_2}5^{b_3}\cdots$, then

$$\begin{aligned}
\alpha\left(\frac{m}{n}\cdot\frac{m'}{n'}\right) &= \alpha((2^{a_1}3^{a_2}5^{a_3}\cdots)\cdot(2^{b_1}3^{b_2}5^{b_3}\cdots)) \\
&= \alpha((2^{a_1+b_1}3^{a_2+b_2}5^{a_3+b_3}\cdots) \\
&= (a_1+b_1, a_2+b_2, a_3+b_3, \dots) \\
&= (a_1, a_2, a_3, \dots) + (b_1, b_2, b_3, \dots) \\
&= \alpha\left(\frac{m}{n}\right) + \alpha\left(\frac{m'}{n'}\right).
\end{aligned}$$

  (There could be some cancelations in components of the sum of the two vectors, but that does not matter. Corresponding cancelations would also happen when we multiply $(m/n)\cdot(m'/n')$ in $\mathbb{Q}^+$.)

- α is onto (surjective) because given an arbitrary element $a = (a_1, a_2, a_3, \dots)$ in H, we can form the product $2^{a_1}3^{a_2}5^{a_3}\cdots$ and the result makes sense as an element m/n of $\mathbb{Q}^+$ because only finitely many of the a_i are different from zero. That means the product is really just a finite product, multiplied by a bunch of 1s. That rational number m/n satisfies $\alpha(m/n) = a$, so α is onto.

- α is one-to-one (injective): Suppose m/n and m'/n' are two elements of $\mathbb{Q}^+$ with

$$\alpha(m/n) = (a_1, a_2, a_3, \dots) = \alpha(m'/n').$$

  We can assume both of the fractions were in lowest terms to start. Then the factorizations of the m, m' give the $a_i > 0$ and the factorizations of the n, n' give the $a_i < 0$. That means that both the numerators and the denominators in the fractions m/n and m'/n' have the same prime factorizations, and that shows they must be equal.

Note: The fancier way of saying the argument α is bijective is to consider the mapping

$$\begin{aligned}
\beta : H &\longrightarrow \mathbb{Q}^+ \\
(a_1, a_2, a_3, \dots) &\longmapsto 2^{a_1}3^{a_2}5^{a_3}\cdots.
\end{aligned}$$

We are really claiming that β is the inverse mapping of α when we consider each element of $\mathbb{Q}^+$ to be represented by a fraction in lowest terms.