Contents

Artin 2.1.5 Consequences of an equation

We are given that $xyz = 1$ in some group G. So

$$yz = x^{-1}$$

and therefore

$$yzx = 1.$$

But it is not necessarily the case that $yxz = 1$. We know $xy = z^{-1}$ but we don't know that this group is abelian.

Artin 2.1.7 Proving that a given binary op is associative

Given the law of composition

$$ab = a,$$

we must prove that

$$(ab)c = a(bc).$$

The LHS becomes

$$(a)c = ac = a$$

while the RHS becomes

$$a(b) = ab = a$$

so it is proved.

Artin 2.2.1 A cyclic matrix group

The elements of the cyclic group generated by

$$\begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}$$

are its powers:

$$\begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

So it's a cyclic group of order 6, isomorphic to the integers modulo 6.

Note that $A^3 = -I$, so $A^6 = I$ is immediate and it's easy to get $A^4 = -A$ and $A^5 = -A^2$ from previously computed powers.

Artin 2.2.15 Uniqueness of identity and inverses in subgroups

(a)

Let e_H be the idenity in H. Then

$$e_H e_H = e_H$$

but since the operation is inherited from G we may multiply by e_H^{-1} in G:

$$e_H^{-1} e_H e_H = e_H^{-1} e_H$$

to get

$$e_G e_H = e_G,$$

that is,

$$e_H = e_G.$$

(b)

Let a^{-H} be the inverse in H and a^{-G} be the inverse in G. Then in H we have

$$aa^{-H} = 1$$

but this equation holds in G as well we may multiply on the left by a^{-G} in G to get

$$a^{-G} aa^{-H} = a^{-G}$$

where the first two factors on the left multiply in G to give the identity, so

$$a^{-H} = a^{-G}.$$

Artin 2.2.20(a) The order of products in abelian groups

Let a, b be elements of an abelian group of orders m, n respectively. Then if $l = \operatorname{lcm}(m, n)$, we see that

$$(ab)^l = a^l b^l = (a^m)^{\frac{l}{m}} (b^n)^{\frac{l}{n}} = 1$$

where all exponents are integers since l is a multiple of both m and n.

But for any element x, we know that $x^y = 1$ implies that its order divides y. So $\operatorname{ord}(ab) \mid \operatorname{lcm}(m, n)$.

(Note that this is NOT a consequence of Lagrange's Theorem.

Here's an incorrect argument: the powers of x from 0 to y (with potential repeat elements) form a group G, and the powers of x from 0 to $\operatorname{ord}(a)$ form a group H, but the order is the smallest number with this property, so all the elements of H are contained in G, so H is a subgroup of G, so $\operatorname{ord}(H) \mid \operatorname{ord}(G)$.

The problem is the repeat elements. For this argument to work, $\operatorname{ord}(G) = y$, but in fact G is the same group as H, so $\operatorname{ord}(G) = \operatorname{ord}(x)$ and we can't conclude from this argument that $\operatorname{ord}(x) \mid y$.)