Artin Reading Group Notes

Jack Ceroni

December 2020

Contents

1 Introduction

The following are notes and solutions for Week 1 of the Artin reading group.

2 Chapter 2: Basic Group Theory

2.1 Recap of Lagrange's Theorem and Related Results

Definition 1. *We define the left coset of a subgroup H of some group G to be the set:*

$$aH = \{ah \mid h \in H\}$$

Note that the collection of cosests forms a partition of G.

Proposition 1. *There exists a bijection from H to aH.*

Proof. We define the map ϕ such that $\phi(h) = ah$. Clearly, such a map is surjective. In addition, we note that if $ah = ah'$, then $h = h'$, which implies that ϕ is injective.

Therefore, ϕ is a bijection, and H and aH have the same number of elements. □

We define $[G : H]$ to be the number of left subgroups of H. It follows that $|G| = |H|[G : H]$ (from above). This leads to Lagrange's theorem.

2.2 Problems

Problem 2.21. Prove that the set of elements of finite order in an Abelian group is a subgroup.

Proof. Given two elements x and y of finite order, we note that there exists m and n such that $x^m = 1$ and $y^n = 1$. Since the group is Abelian, we know that $(xy)^r = x^r y^r$. Therefore:

$$(xy)^{mn} = x^{mn} y^{mn} = (x^m)^n (y^n)^m = 1^n 1^m = 1$$

so xy has finite order as well (namely, mn). Clearly, 1 has finite order, so it is in the group. Finally, for some x of finite order n, we note that:

$$1 = 1^n = (xx^{-1})^n = x^n (x^{-1})^n = (x^{-1})^n$$

so x^{-1} has finite order (namely, n), and is therefore in the group as well. It follows that we have a valid subgroup. □

Problem 3.12. Let G be a group, and let $\phi : G \to G$ be the map $\phi(x) = x^{-1}$. Prove that ϕ is bijective. Then, prove that ϕ is an automorphism if and only if G is Abelian.

Proof. Clearly, ϕ is surjective: given $x \in G$, we note that $\phi(x^{-1}) = x$. In addition, assume that $y^{-1} = x^{-1}$. It follows that:

$$x = xy^{-1}y = xx^{-1}y = y$$

so ϕ is injective. Therefore, ϕ is bijective.

First, assume that ϕ is an automorphism. We then will have:

$$xy = \phi(x^{-1})\phi(y^{-1}) = \phi(x^{-1}y^{-1}) = \phi((yx)^{-1}) = yx$$

so G is Abelian. Now, assume that G is Abelian. We will then have:

$$\phi(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = \phi(x)\phi(y)$$

so ϕ is an automorphism. This completes the proof. □

Problem 4.11. Let G, H be cyclic groups generated by x and y, with orders m and n. What condition must be imposed on m and n such that $\phi(x^i) = y^i$ is a valid homomorphism?

Proposition 2. *$\phi(x^i) = y^i$ is a homomorphism if and only if $m = zn$, where z is a positive integer.*

Proof. First, assume that $m = zn$. We note that in G:

$$x^i = 1x^i = x^{mj}x^i = x^{i+mj}$$

for all integer $j \geq 0$. Clearly, these are the only elements to which x^i is equal in G. Thus, to show that ϕ is a valid map, we must show that x^i and x^{i+mj} are mapped to the same element of H.

We have:

$$\phi(x^i) = y^i$$

and:

$$\phi(x^{i+mj}) = y^{i+mj} = y^i y^{mj} = y^i y^{(zj)n} = y^i$$

so ϕ is a valid map. In addition, we note that:

$$\phi(x^a x^b) = \phi(x^{a+b}) = y^{a+b} = y^a y^b = \phi(x^a)\phi(x^b)$$

Thus, ϕ is a valid group homomorphism.

Conversely, assume that ϕ is a homomorphism. We will have:

$$\phi(x^i) = \phi(x^{i+m}) = \phi(x^i)\phi(x^m) \;\Rightarrow\; \phi(x^m) = y^m = 1$$

Since y has order n, this implies that $m = in$, for some integer $i \geq 0$. This completes the proof. □

Problem 4.23. Let $\phi : G \to G'$ be a surjective homomorphism, and let N be a normal subgroup of G. Prove that $\phi(N)$ is a normal subgroup of G'.

Proof. Consider some element $\phi(n) \in \phi(N)$. Now, let us pick some other element b in G'. Since ϕ is surjective, we note that $b = \phi(a)$. We then have:

$$\phi(a)^{-1}\phi(n)\phi(a) = \phi(a^{-1})\phi(n)\phi(a) = \phi(a^{-1}na)$$

Since N is normal, it follows that $a^{-1}na \in N$, so $\phi(a^{-1}na) \in \phi(N)$. Thus, by definition, $\phi(N)$ is normal as well. □

Problem 5.12. Prove that the non-empty cosets of the kernel of ϕ are the fibres of ϕ.

Proof. Let S be the set of fibres of ϕ. Consider some arbitrary non-empty fibre of the form $\phi^{-1}(a) \in S$.

Let x be an element of the fibre. Now, consider some other element y of the fibre (not necessarily distinct). We note that $\phi(x) = \phi(y) = a$, so it follows that $\phi(y)\phi(x^{-1}) = \phi(yx^{-1}) = 1$. This implies that yx^{-1} is in the kernel, so $y = nx$, for some n in the nullspace.

In addition, clearly, for any element xn, we will have:

$$\phi(xn) = \phi(x)\phi(n) = \phi(x) = a$$

Thus, by definition, each fibre is a coset of the above form.

Note: One way to prove this would be to use a similar procedure to what was done above, by showing that every coset is a fibre. However, we choose a more "crafty" method:

Now, consider some coset xN. Assume that xN is not a fibre. Since cosets partition the set, and each fibre is a coset, it follows that xN cannot intersect any fibre. But $x \in xN$, which would imply that x is not contained in any fibre of ϕ, a contradiction to the fact that fibres partition the domain.

Therefore, each coset must be a fibre.

It follows that the set of cosets is equal to the set of fibres, and the proof is complete. ☐

Problem 7.8. Prove the Correspondence Theorem.

Proof. We define a map that takes each subgroup H containing the kernel of a homomorphism ϕ to $\phi(H)$. We show that such a map defines a bijective correspondence between all subgropus of this form in G, and all subgroups H' of G'.

Consider some subgroup H' of G'. We define the set $\phi^{-1}(H')$. Clearly, $N \in \phi^{-1}(H')$, as $1 \in H'$.

In addition, we note that given $x,\ y \in \phi^{-1}(H')$, we will have $\phi(xy) = \phi(x)\phi(y)$. Clearly, $\phi(x),\ \phi(y) \in H'$, and so too will be $\phi(x)\phi(y)$. Therefore, $xy \in \phi^{-1}(H')$. Similar arguments show that $\phi^{-1}(H')$ contains inverses and the identity. Therefore, $\phi^{-1}(H')$ is a subgroup.

It follows that $\phi(\phi^{-1}(H') \subset H'$ (as ϕ is surjective), and the map that takes H to $\phi(H)$ is surjective.

Now, consider two subgroups that contain N, which we denote A and B. Assume that $\phi(A) = \phi(B)$. Consider some $a \in A$. We note that $\phi(a) = \phi(b)$ for some $b \in B$. But we proved earlier that $a = bn$ for some n in the kernel. We also know that $N \subset B$, so $nb \in B$. This implies that $a \in B$ and $A \subset B$.

Similarly, we can show that $B \subset A$. Therefore, $A = B$. It follows that the map that sends H to $\phi(H)$ is injective, by definition. Now we know that the map is surjective and injective, so it is bijective.

Finally, we note that if H is normal, and given some $g \in \phi(H)$, then:

$$\phi(h)^{-1}\phi(g)\phi(h) = \phi(h^{-1}gh)$$

where $h^{-1}gh$ is in H, as it is normal. Thus, $\phi(h)^{-1}\phi(g)\phi(h) \in \phi(H)$, so $\phi(H)$ is normal as well. This completes the proof. ☐

Proposition 3. *Given some cyclic group generated by x of order n, and some element y of the group, then $y^n = 1$.*

Proof.

$$y^n = (x^m)^n = x^{mn} = (x^n)^m = 1^m = 1$$

☐

Problem 8.3. Prove that a finite cyclic group of order rs is isomorphic to the product of cyclic groups of orders r and s if and only if r and s have no common factors.

Proof. First, assume that C_{rs} is isomorphic to the product of cyclic groups C_r and C_s of orders r and s, so there exists a map $\phi : C_{rs} \ \rightarrow \ C_r \times C_s$. Assume that r and s do share a common factor t. It follows that $r = at$ and $s = bt$, for some a and b.

We then note that $abt = as < rs$, as $a < r$. Since C_{rs} is of order rs, then $x^{abt} \neq 1$ for some x in the group.

Clearly, we must have $\phi(x) = (y,\ z)$, for some y and z. Thus:

$$\phi(x^{abt}) = \phi(x)^{abt} = (y, z)^{abt} = (y^{abt},\ z^{abt}) = ((y^r)^b,\ (z^s)^a) = (1,\ 1)$$

which contradicts the fact that ϕ is injective, as $\phi(1) = (1,\ 1)$ as well.

Now, assume that r and s share no common factors. We define the map that takes x^a in C_{rs} to $(y^a,\ z^a)$ in $C_r \times C_s$.

Clearly, such a map preserves the group operation. In addition, we note that such a rule defines a valid function, as $x^{a+rs} = x^a$ will also be mapped to $(y^a,\ z^a)$.

Given $(y^a,\ z^b)$ in the codomain, we note that $x^s = (y^s,\ 1)$, where $y^s \neq 1$ and $x^r = (1,\ z^r)$ where $z^r \neq 1$. Since the groups are cyclic, we then know that there exist powers to which we can raise y^s to get y^a and z^r to get z^b. Thus, the map is surjective.

In addition, given x^a and x^b such that $\phi(x^a) = \phi(x^b)$. $\square$