Introduction

This document contains solutions to selected problems from Artin's abstract algebra book.

1 Groups

1.1 Laws of Composition

Problem: Let $\mathbb{N}$ denote the set $\{1, 2, 3, \dots\}$ of natural nubmers, and let $s : \mathbb{N} \to \mathbb{N}$ be the *shift* map, defined by $s(n) = n + 1$. Prove that s has no right inverse, but that it has infinitely many left inverses.

1.2 Groups and Subgroups

Problem: Let x, y, z and w be elements of a group G.

a) Solve for y, given that $xyz^{-1}w = 1$.

Solution: x, y, z, w are all elements of G, so therefore an inverse exists for all of them. Given that $xyz^{-1}w = 1$, then we can write $y = x^{-1}w^{-1}z$ by left and right multiplying out inverses. □

---

b) Suppose that $xyz = 1$. Does it follow that $yzx = 1$? Does it follow that $yxz = 1$?

Solution: The first of the two equations follows, since we conclude that $x^{-1} = yz$, and therefore $yzx = (yz)x = x^{-1}x = 1$. The second equation does not follow, since although we conclude that $z^{-1} = xy$ it is not necessarily true that $xy = yx$. □

Problem: In the definition of a subgroup, the identity element in H is required to be the identity of G. One might require only that H have an identity element, not that it need be the same identity in G. Show that if H has an identity at all, then it is the identity in G. Show that the analogous statement is true for inverses.

Solution: The fact about identities is very simple: G has a single identity element, and since H is a subgroup of G, then $H \subset G$, hence the identity element of H must equal the identity element of G.

To be a bit more rigorous, suppose $1_H \neq 1_G$. Then, 1_H is defined such that for all $h \in H$, $h1_H = h$, and since $h \in G$, then we also have $h1_G = h$, so therefore $h1_H = h1_G$, which can only be true if $1_H = 1_G$.

Now consider an element $h \in H$. Since H is a subgroup, then $h^{-1} \in H$, and h^{-1} is defined to be the element that $hh^{-1} = 1$, which also holds in G. Therefore, the inverse of h is the same inverse of h in G. □

1.3 Subgroups of the Additive Group of Integers

Problem: Prove that if a and b are positive integers whose sum is a prime p, their greatest common divisor is 1.

Solution: We have the relation $a + b = p$. Applying modulus, we get:

$$a \equiv p \pmod{b}$$

Since p is prime, then $\gcd(p, b) = 1$ so therefore p^{-1} exists, and we can write $ap^{-1} \equiv 1 \pmod{b}$. This then implies that $a^{-1} \equiv p^{-1} \pmod{b}$, and since a modular inverse exists iff $\gcd(a, b) = 1$, we conclude that $\gcd(a, b) = 1$ from here. □

1.4 Cyclic groups

Problem: An n th root of unity is a complex number z such that $z^n = 1$.

a) Prove that the n-th roots of unity form a cyclic subgroup $\mathbb{C}^\times$ of order n.

Solution: By the fundamental theorem of algebra, we know that the equation $z^n = 1$ has n values. Specifically, we can write the i-th root of unity as:

$$z_i = e^{i\frac{2\pi}{n}}$$

It's clear that each one of these satisfy $z_i^n = 1$, and all n values are distinct, so therefore this set has n elements.

For the properties of a group, starting with closedness:

$$z_i z_j = e^{i\frac{2\pi}{n}} e^{j\frac{2\pi}{n}} = e^{(i+j)\frac{2\pi}{n}}$$

which is another element of the group (if i, j exceed n, it is possible to factor out $e^{2\pi} = 1$ out).

The identity in $C^\times = 1$, which also exists in this subgroup since $1^n = 1$.

As for inverses, for any element z_i, we have:

$$z_i z_{n-i} = e^{i\frac{2\pi}{n}} e^{(n-i)\frac{2\pi}{n}} = e^{n\frac{2\pi}{n}} = 1$$

so the inverse exists. □

---

b) Determine the product of all the n-th roots of unity.

Solution: Since this is a subgroup, each element can be paired up with its inverse, except the identity (whose inverse is itself). Since multiplication is commutative, then the entire product collapses and we get 1. □

Problem: Let x and y be elements of a group G. Assume that each of the elements x, y and xy has order 2. Prove that the set $H = \{1, x, y, xy\}$ is a subgroup of G, and that it has order 4.

Solution: We first show closedness: we know that each element has order 2, so $x^2 = 1$, $y^2 = 1$, $(xy)^2 = 1$, all of which are in H.

Since $x, y \in H$, but $yx \notin H$? How is this a subgroup? □

1.5 Homomorphisms

Problem: Let $\varphi : G \to G'$ be a group homomorphism. Prove that if G is cyclic, then G' is cyclic, and if G is abelian, then G' is abelian.

Solution: Let x be the generator of G, so $\varphi(x) \in G'$ and $\varphi(x^{-1}) = \varphi(x)^{-1} \in G'$. To prove that G' is cyclic, we have $\varphi(x^m) = \varphi(x)^m$ (this follows inductively from the property that $\varphi(ab) = \varphi(a)\varphi(b)$), where m is any integer. Therefore, G' is generated by the element $\varphi(x)$, so therefore G' is cyclic.

Now, if G is abelian, it means that $ab = ba$ for all $a, b \in G$. Therefore, we have $\varphi(ab) = \varphi(a)\varphi(b)$ and $\varphi(ba) = \varphi(b)\varphi(a)$, so we see that $\varphi(a)\varphi(b) = \varphi(b)\varphi(a)$, therefore G' is abelian. □

Problem: Let $f : \mathbb{R}^+ \to \mathbb{C}^\times$ be the map $f(x) = e^{ix}$. Prove that f is a homomorphism, and determine its kernel and image.

Solution: To prove that f is a homomorphism, we prove that $f(ab) = f(a)f(b)$ for $a, b \in \mathbb{R}^+$. Therefore, we're being asked to prove that

$$e^{i(a+b)} = e^{ia}e^{ib}$$

this is obviously true from the laws of exponents, so f is indeed a homomorphism.

The image set is the set $e^{i\theta}$, which is a circle of radius 1 in the complex plane. The kernel is the set of elements in $\mathbb{R}^+$ such that $f(x) = 1$, so this would correspond to the elements $2\pi n$, where n is an integer, since $e^{i2\pi n} = (e^{i2\pi})^n = 1^n = 1$. □

Problem:

a) Let G be a cyclic group of order 6. How many of its elements generate G? Answer the same question for cyclic groups of orders 5 and 8.

Solution: G is a cyclic group of order 6, so if x generates G, then we know that $x^6 = 1$. Now, we claim that if x^n generates G, then $\gcd(n, 6) = 1$. This is required since we need there to exist a value of k such that for all $a \in \{0, \ldots, 5\}$, we have $kn \equiv a \pmod 6$, which is only achievable if n has an inverse.[1] This last condition is true if and only if $\gcd(n, 6) = 1$, so therefore this is a requirement.

Then, this means that all powers coprime to 6 will generate G, so this would be the elements x, x^5.

Since 5 is prime, then it is coprime to all values $\{1, \ldots, 4\}$, so therefore all elements except the identity will generate a cyclic group of order 5.

For order 8, the elements are $\{x, x^3, x^5, x^7\}$. □

---

b) Describe the number of elements that generate a cyclic group of arbitrary order n.

Solution: Building off the previous part, the number of elements is given by $\phi(n)$, where ϕ is Euler's totient function. □

Problem: Prove that the $n \times n$ matries that have the block form $M = \begin{bmatrix} A & B \\ 0 & D \end{bmatrix}$, with A in $GL_r(\mathbb{R})$ and D in $GL_{n-r}(\mathbb{R})$, form a subgroup H of $GL_n(\mathbb{R})$, and that the map $H \to GL_r(\mathbb{R})$ that sends $M \rightsquigarrow A$ is a homomorphism. What is its kernel?

Solution: First, we check that $M \in GL_n(\mathbb{R})$. This is easily shown, by first noticing that we can row reduce D to the identity in the bottom right block, then use it to reduce B to the zero matrix. Then, we reduce A to its identity. Therefore, M is invertible, so $M \in GL_n(\mathbb{R})$.

Next, given $M_1 = \begin{bmatrix} A_1 & B_1 \\ 0 & D_1 \end{bmatrix}$ and $M_2 = \begin{bmatrix} A_2 & B_2 \\ 0 & D_2 \end{bmatrix}$, we compute M_1M_2:

$$M_1M_2 = \begin{bmatrix} A_1A_2 & A_1B_2 + B_1D_2 \\ 0 & D_1D_2 \end{bmatrix} \in GL_n(\mathbb{R})$$

it exists in $GL_n(\mathbb{R})$ by the same argument we did for M. Then, we can also see that $\varphi(M_1M_2) = A_1A_2 = \varphi(M_1)\varphi(M_2)$, so φ is indeed a homomorphism. The kernel is the set of elements in H that are sent to the identity – this is simply the matrices where $A = I$. □

---

[1] This is true because k can be any number, and a can be any number, so we can choose k, a to share factors with 6, at which point the only way a solution exists is $k \equiv an^{-1} \pmod 6$.

1.6 Isomorphisms

Problem: Let G' be the group of real matrices of the form $\begin{bmatrix} 1 & x \\ & 1 \end{bmatrix}$. Is the map $\mathbb{R}^+ \to G'$ that sends x to this matrix an isomorphism?

Solution: An isomorphism is a bijective map between G and G'. This map is indeed bijective, since the unique number x maps to a unique matrix. We now check whether this map φ is a homomorphism:

$$\varphi(x_1)\varphi(x_2) = \begin{bmatrix} 1 & x_1 \\ & 1 \end{bmatrix} \begin{bmatrix} 1 & x_2 \\ & 1 \end{bmatrix} = \begin{bmatrix} 1 & x_1 + x_2 \\ & 1 \end{bmatrix}$$

so we've confirmed that $\varphi(x_1x_2) = \varphi(x_1)\varphi(x_2)$, confirming that φ is an isomorphism. □

Problem: Prove that in a group, the products ab and ba are conjugate elements.

Solution: Our goal is just to show that there exists some $g \in G$ such that $g(ab)g^{-1} = ba$, which can be done by letting $g = a^{-1}$. This is guaranteed to exist in G since $a \in G$. □

Problem: Let H be a subgroup of G, and let g be a fixed element of G. The *conjugate subgroup* gHg^{-1} is defined to be the set of all conjugates ghg^{-1}, with h in H. Prove that gHg^{-1} is a subgroup of G.

Solution: Firstly, $ghg^{-1} \in G$ since all elements are in G, and G is closed under composition. Now, we show closure in H. Let gh_1g^{-1} and gh_2g^{-1} be two elements in H. Then:

$$(gh_1g^{-1})(gh_2g^{-1}) = gh_1(g^{-1}g)h_2g^{-1} = g(h_1h_2)g^{-1}$$

Since H is a subgroup, then $h_1h_2 \in H$, so closedness is guaranteed.

The identity is guaranteed by letting $h = 1_H = 1_G$, so we have $g1_Gg^{-1} = 1_G$.

Now, let $ghg^{-1} \in gHg^{-1}$. Then, the inverse is:

$$(ghg^{-1})^{-1} = gh^{-1}g^{-1}$$

and $h^{-1} \in H$, so the inverse is in gHg^{-1} as well. This concludes the proof. □

1.7 Equivalence Relations and Partitions

Problem: An equivalence relation on S is determined by the subset R of the set $S \times S$ consisting of those pairs (a, b) such that $a \sim b$. Write the axioms for an equivalence relation in terms of the subset R.

Solution: The subset R consists of points (a, b) such that $a \sim b$. Transivity can be expressed as if $(a, b) \in R$ and $(b, c) \in R$ then $(a, c) \in R$, symmetry is $(a, b) \in R \implies (b, a) \in R$, and $\forall a\ (a, a) \in R$. □

1.8 Cosets

Problem: Does every group whose order is a power of a prime p contain an element of order p?

Solution: No. If x is an element of order p, then it implies that the set $\{1, x, \ldots, x^{p-1}\}$ consists of only unique elements, at which point the group is the cyclic group $\langle x \rangle$. Not every group is cyclic, so therefore this is not a requirement. □

Problem: Does a group of order 35 contain an element of order 5? of order 7?

Solution: Due to Lagrange's theorem, the order of every element divides the order of the group, meaning that every element has order 1, 5, 7, 35. If G contains an element x of order 35, then x^7 has order 5 and x^7 has order 5. The identity is the only element with order 1.

Now, suppose G does not have any elements order 7. Then, since every element is order 5, then G consists of n cyclic subgroups each of order 5. Since they all share the identity, then each subgroup contains 4 unique elements.[2] Combining all these subgroups, we get $35 = 4n + 1$, but there is no integer value of n that solves this, so therefore this cannot exist.

A similar argument is made for 7, where we have $6n + 1 = 35$, also with no satisfying value of n. Therefore, G must contain an element of order 5 and 7. □

Problem: Let $\varphi : G \to G'$ be a group homomorphism. Suppose that $|G| = 18, |G'| = 15$, and that φ is not the trivial homomorphism. What is the order of the kernel?

Solution: We know that $|\ker \varphi|$ divides $|G|$, and also that $|G| = |\ker \varphi|\,|\operatorname{im} \varphi|$, and $|\operatorname{im} \varphi|$ divides $|G|$ and $|G'|$. Since $|G'| = 15$, then the only common factor between 18 and 15 is 3, so therefore $|\operatorname{im} \varphi| = 3$. From this, we get $|\ker \varphi| = 6$. □

1.10 The Correspondence Theorem

Problem: Let H and K be subgroups of a group G.

a) Prove that the intersection $xH \cap yK$ of two cosets H and K is either empty or else is a coset of the subgroup $H \cap K$.

Solution: If $xH \cap yK$ is nonempty, then it contains some element z. By (2.8.5), we have that $zH = xH$ and also $zK = yK$ (this is becuase z is in xH and also yK). So, we can simplify our life by only considering WLOG the case where $x = y = z$. Then, we have $z(H \cap K) \subseteq zH \cap zK$, so therefore $zH \cap zK$ contains at least one coset $z(H \cap K)$. Also, $zh = zk$ for some $h \in H$ and $k \in K$, so the only way this can be true is if $h = k \in H \cap K$, so $zH \cap zK \subseteq z(H \cap K)$. Therefore, $zH \cap zK = z(H \cap K)$.

This solution is heavily drawn from stackexchange, make sure you understand it. □

---

b) Prove that if H and K have finite index in G then $H \cap K$ also has finite index in G.

Solution: We know that $H \cap K \subset H$ and $H \cap K \subset K$, so $[G : H \cap K] = [G : H][H : H \cap K]$, and also $[G : H \cap K] = [G : K][K : H \cap K]$. We know $[G : H]$ and $[G : K]$ are finite, so rearranging:

$$[G : H] = \frac{[G : H \cap K]}{[H : H \cap K]} \quad [G : K] = \frac{[G : H \cap K]}{[K : H \cap K]}$$

this implies that the right hand side must be finite, or in other words $[G : H \cap K]$ is finite, so $H \cap K$ is finite in G.

I wonder if there's a way to make this proof slightly better □

Problem: With the notation of the Correspondence Theorem, let H and H' be corresponding subgroups. Prove that $[G : H] = [G' : H']$.

Solution: The Correspondence theorem gives us a bijection between subgroups of H and H', but more importantly it gives us the identity $|H| = |H'||K|$. Further, we know from Lagrange's theorem that:

$$[G : H] = \frac{|G|}{|H|} \quad [G' : H'] = \frac{|G'|}{|H'|}$$

[2] This uses the principle that groups with prime order are cyclic, so if they had any element other than the identity in common, they would be the same cyclic subgroup.

substituting the identity to the right we have:

$$[G' : H'] = \frac{|G'||K|}{|H|}$$

Now, we claim that $|G| = |G'||K|$, but this is a direct result of $|G| = |\operatorname{im}\varphi||\ker\varphi|$, so the desired result immediately follows. [3] □

1.12 Quotient Groups

Problem: Show that if a subgroup H of a group G is not normal, there are left cosets aH and bH whose product is not a coset.

Solution: Since H is not normal, there exists some $g \in G$ and $h \in H$ such that $ghg^{-1} \notin H$. Also, $(aH)(bH)$ is the set of elements $ahbh'$ for $h, h' \in H$.

Now let $a = g, b = g^{-1}$, our product set is $(aH)(bH) = ghg^{-1}h'$ for all $h, h' \in H$. Now, let $h_0 \in G$ be the element such that $gh_0g^{-1} \notin H$, then we can let $h' = 1$, implying that $gh_0g^{-1} \in (gH)(g^{-1}H)$. Now, letting $h = 1$ leaves us with h', so $H \subset (gH)(g^{-1}H)$.

If $(gH)(g^{-1}H)$ is a coset of H (since cosets partition G and $ab \in (aH)(bH)$), then it has $|H|$ elements, since all cosets have the same order. Combining this with $H \subset (gH)(g^{-1}H)$ allows us to conclude that $H = (gH)(g^{-1}H)$, but then we get that $gh_0g^{-1} \in H$, which is a contradiction since H is not normal. □

Problem: In the general linear group $GL_3(\mathbb{R})$, consider the subsets

$$H = \begin{bmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{bmatrix}, \text{and } K = \begin{bmatrix} 1 & 0 & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

where $*$ represents an arbitrary real number. Show that H is a subgroup of GL_3, that K is a normal subgroup of H, and identify the quotient group H/K. Determine the center of H.

Solution: H is the set of upper triangular matrices with entries 1 on the diagonal. We know that two upper triangular matrices multiplied together give an upper triangular matrix, so H is closed under composition. The identity element is in H, where all non-diagonal elements are zero. The inverse is also upper triangular (this is not hard but I really don't want to prove it), all of which combined means that H is a subgroup.

Now, consider any element of H, and an element $h \in H$, written as follows:

$$h = \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} \quad h^{-1} = \begin{bmatrix} 1 & -x & -y + xz \\ 0 & 1 & -z \\ 0 & 0 & 1 \end{bmatrix}$$

Then, doing the computation:

$$hkh^{-1} = \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & w \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -x & -y + xz \\ 0 & 1 & -z \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & w \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \in K$$

so therefore K is a normal subgroup of H. The quotient group H/K is the set of cosets of K, so it's the set of matrices of the form:

$$\begin{bmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{bmatrix}$$

[3] Another way to see this is that every element in $g' \in G'$ that has a non-kernel pre-image $g \in G$ is also mapped to g' by gk, where $k \in K$, so for every element in G' there are $|K|$ kernel elements that are collapsed, hence the multiplication.

so H/K is actually just H itself. The center of H are the matrices in $GL_3(\mathbb{R})$ that do commute with matrices in H; since matrices don't commute in general, there are two matrices that come to mind: the identity and the zero matrix. □

Problem: Let G be the group of upper triangular real matrices $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$ with a and d different from zero. For each of the following subsets, determine whether or not S is a subgroup, and whether or not S is a normal subgroup. If S is a normal subgroup, identify the quotient group G/S.

i) S is the subset defined by $b = 0$.

ii) S is the subset defined by $d = 1$.

iii) S is the subset defined by $a = d$.