Annotations : A first course in abstract algebra, 7th Edition, John B. Fraleigh

Jacob Antony
jacobantony987@gmail.com

December 26, 2020

Sets and Relations

pp. 15 **There is exactly one set with no elements.**

Any two sets with no elements are equal. Thus the empty set, is the trivial subset of any set.

pp. 16 **Every definition is an if and only if type of statement**

Definitions are the first among the if and only if statements. We can afford only one definition for an object. Thus equivalent if and only if statements are characterisations and are potential definitions.

Chapter 1

Groups and Subgroups

. . . Thus H is not closed under addition. §2.6 pp. 35

$H = \{0, 1, 4, 9, \cdots\}$. When we add two element of H, say $1 + 4$, we are not getting an element of H. Thus H is not closed under addition. In other words, you can't add two numbers in H.

. . . $*$ is not everywhere defined on $\mathbb{Q}$. §2.19 pp. 39

Given $a * b = a/b$. Then $2 * 0$ is undefined. Thus $*$ is not well-defined on $\mathbb{Q}$.

. . . we showed that . . . $< U, \cdot >$ and $< \mathbb{R}_c, +_c >$ are isomorphic . . . and $< U_n, \cdot >$ and $< \mathbb{Z}_n, +_n >$ are isomorphic . . . §3.7 pp. 44

Let the points on the unit circle U be of the form $e^{i\theta}$ where $0 \leq \theta < 2\pi$ and the points on the line segment $\mathbb{R}_c$ be of the form x where $0 \leq x < c$. Define a function $\phi : U \to R_c$ such that $\phi(e^{i\theta}) = \frac{c\theta}{2\pi}$. Clearly, ϕ is a bijection and

$$\phi(e^{i\theta_1} \cdot e^{i\theta_2}) = \phi(e^{i(\theta_1+\theta_2)}) = c\frac{\theta_1 +_{2\pi} \theta_2}{2\pi} = c(\frac{\theta_1}{2\pi} +_1 \frac{\theta_2}{2\pi}) = \frac{c\theta_1}{2\pi} +_c \frac{c\theta_2}{2\pi} = \phi(e^{i\theta_1}) +_c \phi(e^{i\theta_2})$$

And thus ϕ is a homomorphism.

Let the nth roots of unity be of the form $e^{ik\frac{2\pi}{n}}$ where $0 \leq k < n$ and set $\mathbb{Z}_n = \{0, 1, \cdots, (n-1)\}$. Define a function $\phi : U_n \to \mathbb{Z}_n$ such that $\phi(e^{ik\frac{2\pi}{n}}) = k$. Clearly, ϕ is a bijection and a homomorphism.

$$\phi(e^{ik\frac{2\pi}{n}} \cdot e^{im\frac{2\pi}{n}}) = \phi(e^{i(k+m)\frac{2\pi}{n}}) = k +_n m = \phi(e^{ik\frac{2\pi}{n}}) \ +_n \ \phi(e^{im\frac{2\pi}{n}})$$

Exercise 27 asks . . . for a collection of binary algebraic structures, the relation $\simeq$ . . . is an equivalence relation . . . §3.7 pp. 44

Let A, B, C be three binary algebraic structures.

1. The identity map $i : A \to A$ is an isomorphism.

2. Let $\phi : A \to B$ be an isomorphism, then $\phi^{-1} : B \to A$ is also an isomorphism.

3. Let $\phi : A \to B$, $\psi : B \to C$ be isomorphisms, then $\psi \circ \phi : A \to C$ is an isomorphism.

Thus the isomorphism relation is an equivalence relation on binary algebraic structures.

§3.10 pp. 45 **A structural property of a binary algebraic structure is one that must be shared by any isomorphic structure.**

We say that a property is structral if isomorphic structures agree on them. Associativity is structural implies that 1. if a binary algebraic structure is associative, all binary algebraic structures isomorphic to it are associative and 2. if a binary algebraic structure is non-associative, then all binary algebraic structures isomorphic to it are non-associative.

§3.15 pp. 47 **. . . We have exhibited a structural property that distinguishes these two structures.**

Proving that there doesn't exists an isomorphism between two structures is a hard task. At times, it is easier to show that two binary structures doesn't share a structural property. And we know that, this wouldn't happen unless they are non-isomorphic.

In the above case, $< \mathbb{Q}, + >$ and $< \mathbb{Z}, + >$ are non-isomorphic. The equation $x + x = c$ has a solution x for all $c \in \mathbb{Q}$. However, $x + x = c$ doesn't have a solution $x \in \mathbb{Z}$ for $c = 3 \in \mathbb{Z}$. Thus, the existence of solution for linear equations is a structral property that distinuguishes $\mathbb{Q}$ from $\mathbb{Z}$.

§4.13 pp. 54 $GL(n, \mathbb{R}) \simeq GL(\mathbb{R}^n)$

$GL(n, \mathbb{R})$ is the general linear group of degree n which is the set of all invertible $n \times n$ matrices with real entries. $GL(\mathbb{R}^n)$ is the set of all invertible linear transformations from $\mathbb{R}^n$ onto $\mathbb{R}^n$. The isomorphism comes from the context of linear algebra.

We have an isomophism $\phi : GL(n, \mathbb{R}) \to GL(\mathbb{R}^n)$ defined by $\phi(a_{ij}) = T$ such that $T(\epsilon_j) = (a_{1j}, a_{2j}, \cdots, a_{nj})$ where $\epsilon_j = (\delta_{1j}, \delta_{2j}, \cdots, \delta_{nj})$.

The isomorphism $\phi : GL(n, \mathbb{R}) \to GL(\mathbb{R}^n)$ correpsonds to the standard ordered basis $\{\epsilon_1, \epsilon_2, \cdots, \epsilon_n\}$ of vector space $\mathbb{R}^n$ over the field $\mathbb{R}$. And thus the set of all isomorphisms from $GL(n, \mathbb{R})$ onto $GL(\mathbb{R}^n)$ is isomorphic to the set of all ordered basis for the vector space $\mathbb{R}^n(\mathbb{R})$.

pp. 59 **There is only one group of three elements, up to isomorphism.**

Consider any two groups of order 3. They are isomorphic.

§5.4 pp. 64 **If a subset H of a group G is closed under the binary operation**

of G and if H with the induced operation from G is itself a group, then H is a subgroup of G.
Suppose G is a group. Then G is a nonempty set and the binary operation $*$ on G satisfies the group axioms. Suppose H is a subset of the set G. If $*$ on any two elements of H gives an element of H, then H is closed under the operation $*$. If H with this induced operation $*$ is a group, then H is a subgroup of G.

A subset of G with some other operation may also form a group. Such groups are not considered as subgroups.

There are two different types of group structures of order 4. §5.9 pp. 65
Any group of order 4 is either isomorphic to group V or group $\mathbb{Z}_4$.

Let G be the multiplicative group of all invertible $n \times n$ matrices with entries in $\mathbb{C}$ and let T be subset of G consisting of those matrices with determinant 1. ... T is a subgroup of G. §5.16 pp. 67
$G \simeq GL(n, \mathbb{C})$ and $T \simeq SL(n, \mathbb{C})$.

... let $n\mathbb{Z}$ be the cyclic subgroup $<n>$ of $\mathbb{Z}$. §5.22 pp. 68
Group $\mathbb{Z}$ is the additive group of integers. And $n\mathbb{Z}$ is the subgroup of $\mathbb{Z}$ generated by n. For example : The set of all even integers, $2\mathbb{Z}$.

Every cyclic group is abelian. §6.1 pp. 73

A subgroup of a cyclic group is cyclic. §6.6 pp. 75

The subgroups of $\mathbb{Z}$ are precisely the groups $n\mathbb{Z}$ ... §6.7 pp. 75
Subgroups of cyclic groups are cyclic. And the cyclic subgroups of $\mathbb{Z}$ with generator n is $n\mathbb{Z}$.

Let G be a cyclic group with generator a. If the order of G is infinite, then G is isomorphic to $<\mathbb{Z}, +>$. If G has finite order, then G is isomorphic to $<\mathbb{Z}_n, +_n>$. §6.10 pp. 77
The cardinality of $\{a^n : n \in \mathbb{Z}\}$ is atmost $\aleph_0$. Thus every cyclic group is countable.

Let G be a cyclic group with n elements and generated by a. Let $b \in G$ and $b = a^s$. Then b generates a cyclic subgroup H of G containing n/d elements, where d is the greatest common divisor of n and s. Also $<a^s>=<a^t>$ if and only if $\gcd(s, n) = \gcd(t, n)$. §6.14 pp. 78
For example : $4 \in \mathbb{Z}_{10}$ has order $\gcd(4, 10) = 2$. Also $<4>\simeq<8>$.

If a is a generator of a cyclic group of order n, then the other generators of G are the elements of the forms a^r, where r is relatively prime to n. §6.16 pp. 79
For example : $\mathbb{Z}_{18}$ has $\phi(18) = 6$ generators.

Subgroup diagram of $\mathbb{Z}_{18}$ §6.18 pp. 79
Collection of subgroups of $\mathbb{Z}_n$ forms a lattice.

Suppose we want to find as small a subgroup as possible that §7 pp.82

contains both a and b . . . $a^2b^4a^{-3}b^2a^5$ . . . we cannot "simplify" . . . since G may not be abelian.

Algorithm to find the order of a finitely generated subgroup of $SL(n, \mathbb{C})$.

§7.5 pp. 83 **If there is a finite set $\{a_i : i \in I\}$ that generates G, then G is finitely generated.**

Every finitely generated group has countable order. The group $<\mathbb{Q}, +>$ is a countable group which cannot be finitely generated.

Chapter 2

Permutations, Cosets and Direct Products

Each element of $GL(2,\mathbb{R})$ yields a transformation of the plane $\mathbb{R}^2$ into itself. §8 pp. 89

Nature of transformations yielded by $SL(2,\mathbb{R})$

Characterise contractions from $\mathbb{R}^2$ into itself

Characterise fixed points of transformations

A permutation of a set is a function $\phi : A \to A$ that is both one to one and onto. §8.3 pp. 90

Permuations are bijections.

If sets A and B have the same cardinality, then $S_A \simeq S_B$. §8.7 pp. 92

Permutation group depends only on the cardinality of the set.

S_3 has the minimum order for any nonabelian group. §8.7 pp. 93

Every group of order 2,3,4 and 5 are abelian. And there is only one non-abelian group of order six upto isomophism.

Let G and G' be groups and let $\phi : G \to G'$ be a one-to-one function such that $\phi(xy) = \phi(x)\phi(y)$ ... Then $\phi[G]$ is a subgroup of G' ... and ϕ provides an isomorphism of G and $\phi[G]$. §8.15 pp. 96

Every group is isomorphic to a group of permutations. §8.16 pp. 96

The map ϕ ... is the left regular representation of G, and the map μ ... is the right regular representation of G. §8.17 pp. 97

$\phi : G \to S_G$, $\phi(x) = \lambda_x$ where $\lambda_x : G \to G$, $\lambda_x(g) = xg$. Thus $G \simeq \phi[G]$.

$\mu : G \to S_G$, $\mu(x) = \rho_{x^{-1}}$ where $\rho_x : G \to G$, $\rho_x(g) = gx$. Thus $G \simeq \rho[G]$.

Let H be a subgroup of a finite group G. Then the order of H is a divisor of the order of G. §10.10 pp. 114

Every group of prime order is cyclic. §10.11 pp. 114

The order of an element of a finite group divides the order of the group. §10.12 pp. 115

§10.14 pp. 115 **Suppose ... $K \leq H \leq G$, and suppose $(H : K)$ and $(G : H)$ are both finite. Then $(G : K)$ is finite and $(G : K) = (G : H)(H : K)$.**
H divides G into G/H cosets. And K divides H into H/K cosets. Thus K divies each H coset into G/K cosets. Thus, K divides G into $G/H \times H/K = G/K$ cosets.

§12 pp. 128 **Given any subset S of $\mathbb{R}^2$, the isometries of $\mathbb{R}^2$ that carry S onto itself ... is the group of symmetries of S in $\mathbb{R}^2$.**

S12 pp. 128 **It can be proved that every isometry of the plane is one of just four types ... translation ... rotation ... reflection ... glide reflection ...**
Every combination of those four isometries is one among these four or an identity map.

§12.5 pp. 129 **Every finite group G of isometries of the plane is isomorphic to either $\mathbb{Z}_n$ or to a dihedral group D_n for some positive integer n.**

§12 pp. 130 **A discrete frieze consists of a pattern of finite width and height that is repeated endlessly in both directions along its baseline ... those isometries that carry each basic pattern onto itself or onto another instance of the pattern ... frieze group.... Each group obtained can be shown to be isomorphic to one of $\mathbb{Z}$, D_∞, $\mathbb{Z} \times \mathbb{Z}_2$, or $D_\infty \times \mathbb{Z}_2$.**

§12 pp. 131 **... study of symmetries when a pattern ... is repeated by translations ... to fill the entire plane.... wallpaper groups or or the plane crystallographic groups.... there are 17 different types of wallpaper patterns ...**

Chapter 3

Homomorphism and Factor Groups

Let F be ... all functions mapping $\mathbb{R}$ onto $\mathbb{R}$ .... Let $\phi_c : F \to \mathbb{R}$ be the evaluation homomorphism defined by $\phi_c(f) = f(c)$ ... §13.4 pp. 140
The function ϕ_c evaluates each function $f \in F$ at real number c.

Let G ... be a direct product of groups. The projection map $\pi_i : G \to G_i$ where $\pi_i(g_1, g_2, \cdots, g_n) = g_i$ is a homomorphism ... §13.8 pp. 141
The direct product group, $G = G_1 \times G_2 \times \cdots \times G_n$ can be imagined as an n-dimensional space with G_i as ith co-ordinate axis. Then projection map π_i of points in n-dimensional space G are their shadows on the ith axis.

Let ϕ be a homomorphism of a group G into a group G'. ... ϕ preserves identity element, inverses and subgroups. §13.12 pp. 142

Let $\phi : G \to G'$ be a homomorphism of groups. The subgroup $\phi^{-1}[\{e'\}] = \{x \in G : \phi(x) = e'\}$ ... is the kernel of ϕ ... §13.13 pp. 143
Homomorphism ϕ carries a subgroup of G into the trivial subgroup of G'.

Let $\phi : G \to G'$ be a group homomorphism, and let $H = \ker(\phi)$ ... $\phi^{-1}[\phi(a)]$ is the left coset aH ... and ... right coset Ha ... §13.15 pp. 144

A group homomorphism $\phi : G \to G'$ is a one-to-one map if and only if $\ker(\phi) = \{e\}$ §13.18 pp. 145

A subgroup H of a group G is normal if its left and right cosets coincide ... $gH = Hg$ for all $g \in G$. §13.19 pp. 146

If $\phi : G \to G'$ is a group homomorphism, then $\ker(\phi)$ is a normal subgroup of G. §13.20 pp. 146

Let $\phi_i : G_i \to G_1 \times G_2 \cdots \times G_r$ be given by $\phi_i(g_i) = (e_1, e_2, \cdots, g_i, \cdots, e_r)$ ... is an injection map ... §13.E7 pp. 147

Let $\phi : G \to G'$ be a group homomorphism with kernel H. Then the cosets of H form a factor group.... Also, the map $\mu : G/H \to \phi[G]$ defined by $\mu(aH) = \phi(a)$ is an isomorphism.... §14.1 pp. 151

§14.6 pp. 153 **The group G/H ... is the factor group ... of G by H.**
Kernel of every group homomorphism $\phi : G \to G'$ is a normal subgroup H of G. And there is a factor group G/H of G for every group homomorphism.

§14.9 pp. 153 **Let H be a normal subgroup of G. Then $\gamma : G \to G/H$ given by $\gamma(x) = xH$ is a homomorphism with kernel H.**
The homomorphism from group G into its factor group G/H.

§14.11 pp. 154 **Let $\phi : G \to G'$ be a group homomorphism with kernel H. Then $\phi[G]$ is a group, and $\mu : G/H \to \phi[G]$ given by $\mu(gH) = \phi(g)$ is an isomorphism. If $\gamma : G \to G/H$ is the homomorphism given by $\gamma(g) = gH$, then $\phi(g) = \mu\gamma(g)$ for each $g \in G$.**