An Introduction to the Theory of Groups

Joseph J. Rotman

April 9, 2018

Fourth Edition

Problems

Chapter 1

1.13

(i) A permutation $\alpha \in S_n$ is ***regular*** if either α has no fixed points and it is the product of disjoint cycles of the same length, or $\alpha = \mathbb{1}$. Prove that α is regular iff it is a power of an n-cycle β; that is, $\alpha = \beta^m$ for some m. (*Hint:* if $\alpha = (a_1 a_2 \dots a_k)(b_1 b_2 \dots b_k) \dots (z_1 z_2 \dots z_k)$, where there are m letters a, b, ..., z, then let $\beta = (a_1 b_1 \dots z_1 a_2 b_2 \dots z_2 \dots a_k b_k \dots z_k)$.)

Solution: β^m takes a_1 through $b_1 \dots z_1$ to a_2 as desired. $\mathbb{1}$ can be expressed as β^n for $\beta(j) = j+1$ an n-cycle. For a general regular α, disjointess of the sets a_j, b_j, ...z_j guaranteed that the β from the hint is an n-cycle. If there's some n-cycle β with $n = mk$, and we take the mth power, we also get m disjoint, length-k cycles, as desired.

(ii) If α is an n-cycle, then α^k is a product of $\gcd(n,k)$ disjoint cycles, each of length ${}^{n}/_{\gcd(n,k)}$.

Solution: $\alpha^n = \mathbb{1}$. If n is a multiple of k, then $\alpha^n = \left(\alpha^k\right)^{n/k}$. α^k would then be a product of k ${}^{n}/_{k}$-cycles. In the case where n is not a multiple of k, but they have a non-trivial gcd, then starting at α_0, α would take us to α_1. α^k will take us to α_k. It takes α_k to α_{2k}, and so on until we get to $\alpha_{mk} = \alpha_0$. This happens if $m = \frac{n}{\gcd(n,k)}$, but I don't know how to prove that.

(iii) If p is prime, then every power of a p cycle is either a p-cycle or $\mathbb{1}$.

Solution: This is a corollary of the last exercise, noting that $\gcd(p,k) = 1$ if $k \neq p$ and p if $k = p$.

1.17 How many $\alpha \in S_n$ are there with $\alpha^2 = \mathbb{1}$?

Solution: There's $\mathbb{1}$, and there's disjoint unions of transpositions. In terms of single transpositions, there are $\binom{n}{2}$ of them. If I'm going to put together a product of j transpositions, there are $\binom{n}{2}$ ways to choose the first transposition, $\binom{n-2}{2}$ ways to choose the second, and $\binom{n-2j}{2}$ ways to choose the jth. Since any permutation of these transpositions is equivalent, I ought to get

$$1 + \sum_{j=1}^{n/2} \frac{1}{j!} \prod_{k=0}^{j} \binom{n-2k}{2}$$

or something, it's not important.

1.26 A group for which $x^2 = \mathbb{1}$ for all x must be Abelian.

Solution: We know that $aa = aea = abba = \mathbb{1}$, and that $abab = \mathbb{1}$. This implies that ab and ba must both be equal to $b^{-1}a^{-1}$.

1.27

(i) Let G be a finite abelian groupcontaining no elements $a \neq e$ with $a^2 = e$. Evaluate $a_1 * a_2 * \ldots * a_n$, where $a_1, a_2, \ldots, a_n$ is a list of all elements in G with no repetitions.

Solution: Just for laughs, let's invert this big element. From the result of Exercise 1.23, we get $(a_1 * a_2 * \ldots * a_n) = a_n^{-1} * a_{n-1}^{-1} * \ldots * a_1^{-1}$. Let A be another name for this big element, so I don't have to LaTeXit all out. The inverses of the individual group elements are unique elements of the group themselves, so the inverse of A is another product of all elements of the group. G is abelian, so $A^{-1} = A$, since all permutations of products are equivalent. This means $A^2 = e$, and the only element of G for which that holds is $\mathbb{1}$.

(ii) Prove ***Wilson's Theorem***: If p is prime, then

$$(p-1)! = -1 \mod p.$$

(*Hint:* The nonzero elements of $\mathbb{Z}_p$ form a multiplicative group.)

Solution: As far as I'm concerned, this completely contradicts the last exercise, since -1 is not the multiplicative identity unless $p = 2$. One interesting thing to note is that $(-1)^2 = 1 = 1^2$, violating the assumption of part (i). Now things start to get a little clearer. The inverse is unique, so, for all numbers from 2 up to $p-2$, the multiplicative inverse mod p is *also* in the set `range`$(2, p-1)$ (ranges are taken to be Python-style). That means that $(p-2)! = \mathbb{1}$, and $(p-1)! = p-1$, as desired.

1.31 Let G be a group, let $a \in G$, and let m and n be relatively prime integers. If $a^m = \mathbb{1}$, show that there exists a b such that $a = b^n$. (*Hint:* There are integers s and t such that $sm + tn = 1$.)

Solution: (Special thanks to Joel Klassen and Christophe Vuillot for their assistance.) We know $a^m = \mathbb{1}$, so that $a^{m+1} = a$. From the hint, $a^{m+sm+tn} = a$, and we can cancel multiples of m to obtain $a^{tn} = a$, so we set $b = a^t$ and get what we were after.

1.42 Let $G = \{x_1, x_2, \ldots, x_n\}$ be a set equipped with an operation $*$, let $A = [a_{ij}]$ be its multiplication table (i.e. $a_{ij} = x_i * x_j$), and assume that G has a two-sided identity e: $e * x = x * e = x$ for all $x \in G$.

(i) Show that $*$ is commutative if and only if A is symmetric.

Solution: This is true by definition.

(ii) Show that every element $x \in G$ has a (two-sided) inverse (i.e. there is an $x' \in G$) such that $x' * x = x * x' = e$. if and only if A is a ***Latin Square*** (i.e. all rows and columns are permutations of G).

Solution: (Thanks to Joel Klassen and Christophe Vuillot for basically doing this problem for me). If A is a Latin Square, then there exists a left inverse and a right inverse for x, since $\mathbb{1}$ must appear in the row and column corresponding to x. $zx = \mathbb{1}$, $xy = \mathbb{1}$, therefore $zxy = z$, but $zx = \mathbb{1}$, so $y = z$.

Likewise, if A is not a Latin square, then there are different elements y and z such that $xy = xz = w$. If x has a left inverse, then $y = z$ and we have a contradiction. If it doesn't, we've proven what we want to prove.

(iii) Assume that $e = x_1$ so that the first row of A has $a_{1i} = x_i$. Show that the first column of A has $a_{i1} = x_i^{-1}$ for all i if and only if $a_{ii} = \mathbb{1}$ for all i.

Solution: This is mad trivial.

(iv) With the multiplication table as shown in (iii), show that $*$ is associative if and only if $a_{ij}a_{jk} = a_{ik}$.

Solution:

If: The trick here is that, if the matrix is arranged such that $\mathbb{1}$ is on the diagonal, then $a_{ij} = x_i x_j^{-1}$. If multiplication is associatve, $a_{ij}a_{jk} = x_i x_j^{-1} x_j x_k^{-1} = x_i x_k^{-1} = a_{ik}$, $\blacksquare$.

Only If: Every x_k can be expressed as $x_i x_j^{-1}$ for fixed x_i, since the multiplication table is a latin square. This implies that the product of three elements $x_k x_l x_m = x_i x_j^{-1} x_j x_n^{-1} x_n x_o^{-1} = a_{ij}a_{jn}a_{no}$. We can evaluate this product in either order, using the assumed product: $a_{ij}a_{jn}a_{no} = a_{in}a_{no} = a_{ij}a_{jo} = a_{io}$, $\blacksquare$.

2.3 The set-theoretic union of two subgroups is a subgroup if and only if one is contained in the other. Is this true if we use three subgroups?

Solution: No, see Bruckheimer et al, 1970: `https://www.jstor.org/stable/pdf/2316854.pdf`.

2.4 Let S be a proper subgroup of G. If $G - S$ is the complement of S, prove that $\langle G - S \rangle = G$.

Solution: We know that $\langle G - S \rangle$ contains $G - S$, so all we have to prove is that the elements of S can be generated by multiplying together two things in $G - S$. Pick an element of $G - S$ g. $g^{-1} \notin S$, since that would contradict the inclusion of the inverse. Also, $sg^{-1} \notin S$ for any $s \in S$, since that would contradict closure. However, $sg^{-1} \cdot g = s$, so we can find two elements of $G - S$ that generate s under multiplication.

2.5 Let $f : G \to H$ and $g : G \to H$ be homomorphisms, and let

$$K = \{a \in G : f(a) = g(a)\}.$$

Must K be a subgroup of G?

Solution: We need:

- the identity to be in the set. This is guaranteed by Theorem 1.13 – $f(\mathbb{1}) = \mathbb{1}'$, so $\mathbb{1} \in K$.
- closure under the inverse. This is also guaranteed by Theorem 1.13 – $f(a^{-1}) = f(a)^{-1} = g(a)^{-1} = g(a^{-1})$.
- closure under multiplication. This is guaranteed by the defining property of the homomorphism– $f(ab) = f(a)f(b) = g(a)g(b) = g(ab)$.

K is a subgroup. $\blacksquare$

2.7 If $n > 2$, then A_n is generated by all the 3-cycles. (*Hint:* $(ij)(jk) = (ijk)$ and $(ij)(kl) = (ijk)(jkl)$).

Solution: Parity is defined as the number of transpositions in a decomposition of a permutation. For each adjacent pair of transpositions in such a decomposition, we can apply one of the two formulae in the hint to express it as a product of 3-cycles.