Chapter 2 Exercises
Gallian's Book on Abstract Algebra

Spencer T. Parkin

January 29, 2014

Problem 1

Give two reasons why the set of odd integers under addition is not a group.

We have no closure and no identity element.

Problem 2

Referring to Example 13, verify the assertion that subtraction is not associative.

$$(a-b)-c = a-b-c \neq a-b+c = a-(b-c)$$

Problem 3

Show that $\{1,2,3\}$ under multilication modulo 4 is not a group but that $\{1,2,3,4\}$ under multilication modulo 5 is a group.

Notice that $2^2 \equiv 0 \pmod 4$ and $0 \notin \{1,2,3\}$.

Notice that $\{1,2,3,4\} = U(5)$ is a group by Problem 35 below.

Problem 6

Given an example of group elements a and b with the property that $a^{-1}ba \neq b$. In D_4, we have

$$R_{270}HR_{90} = V.$$

Problem 8

Show that the set $\{5, 15, 25, 35\}$ is a group under multiplication modulo 40. What is the identity element of this group? Can you see any relationship between this group and $U(8)$.

The Caylay table shows that it is a group with identity element 25. The Caylay table for $\{5, 15, 25, 35\}$ can be found by multiplying all entries in the Caylay table for $U(8)$ by 5. The groups are isomorphic.

Problem 11

Prove that the set of all 2×2 matrices with entries from $\mathbb{R}$ and determinant $+1$ is a group under matrix multiplication.

We have closure by the property of determinants. For matrices A and B, this is given by

$$1 = (\det A)(\det B) = \det AB.$$

Matrix mulltiplication is associative. The identity matrix is the group identity. All matrices with non-zero determinants have inverses.

Problem 12

For any integers $n > 2$, show that there are at least two elements in $U(n)$ that satisfy $x^2 = 1$.

Clearly $1 \in U(n)$ satisfies this. Now consider $n - 1 \in U(n)$.

$$(n-1)^2 = n^2 - 2n + 1 \equiv 1 \pmod{n}$$

Problem 14

Let G be a group with the following property: Whenever a, b and c belong to G and $ab = ca$, then $b = c$. Prove that G is Abelian. ("Cross" cancellation implies commutativity.)

Let $x = ba$ for two elements $a, b \in G$. It follows that $ax = aba$. Then, by "cross" cancelation, we get $x = ab$. We now see that $ba = x = ab$.

Problem 15

(Law of Exponents for Abelian Groups) Let a and b be elements of an Abelian group and let n be any integer. show that $(ab)^n = a^n b^n$. Is this also true for non-Abelian groups?

Clearly this holds for the case $n = 1$, even in non-Abelian groups. Assume it holds for the case $n - 1 \geq 1$. Then $(ab)^n = (ab)^{n-1}ab = a^{n-1}b^{n-1}ab$ by our inductive hypothesis. Then, since our group is Abelian, we have $a^{n-1}b^{n-1}ab = a^n b^n$.

In a non-Abelian group, consider the case $n = 2$, and let a and b be non-commuting members of the group. Then if $abab = aabb$, it follows by the cancelation property that $ab = ba$, which is a contradiction. Therefore, $abab \neq aabb$. It follows that the equation $(ab)^n = a^n b^n$ does not generaly hold for non-Abelian groups.

Problem 16

(Socks-Shoes Property) In a group, prove that $(ab)^{-1} = b^{-1}a^{-1}$. Find an example that shows that it is possible to have $(ab)^{-2} \neq b^{-2}a^{-2}$. Find distinct nonidentity elements a and b from a non-Abelian group with the property that $(ab)^{-1} = a^{-1}b^{-1}$. Draw an analogy between the statement $(ab)^{-1} = b^{-1}a^{-1}$ and the act of putting on and taking off your socks and shoes.

Notice that, by associativity, we have $ab(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = e$.

Now notice, letting $x = a^{-1}$ and $y = b^{-1}$, that while $(ab)^{-2} = ((ab)^{-1})^2 = (b^{-1}a^{-1})^2 = b^{-1}a^{-1}b^{-1}a^{-1} = yxyx$, we have $b^{-2}a^{-2} = (b^{-1})^2(a^{-1})^2 = b^{-1}b^{-1}a^{-1}a^{-1} = yyxx$. It then follows, by Problem 15, that distinct nonidentity and non-commuting elements taken from a non-Abelian group can be found such that $(ab)^{-2} \neq b^{-2}a^{-2}$. Knowing that it exists, I don't feel a need to find any one particular example.

I fail to see the analogy.

Problem 17

Prove that a group G is Abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$.

Letting $x = a^{-1}$ and $y = b^{-1}$, suppose $(ab)^{-1} = xy$. Then $xy = (ab)^{-1} = b^{-1}a^{-1} = yx$.

Now suppose G is Abelian. Then $(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}$.

Problem 18

In a group, prove that $(a^{-1})^{-1} = a$ for all a.

Let $x = a^{-1}$. We must show that $x^{-1} = a$. To that end, we have

$$xa = e \implies x^{-1}xa = x^{-1} \implies a = x^{-1}.$$

Problem 23

Prove that every group table is a Latin square.

If the Caylay table for a group G is not a Latin square, then there exist elements $a, b, c \in G$ such that $b \neq c$, yet $ab = ac$. But all groups have the cancelation property, so that $ab = ac \implies b = c$, which is a contradiction. The Caylay table, therefore, must be a Latin square.

Problem 29

Let G be a finite group. Show that the number of elements of x of G such that $x^3 = e$ is odd. Show that the number of elements x of G such that $x^2 \neq e$ is even.

Clearly $e^3 = e$ so that there is always at least one such element. Suppose now that $x \in G$ is not e and that $x^3 = e$. Now notice that the inverse of x is its square and that $x^2 \neq x$, since $x^2 = x \implies x = e$. Now notice that if we let $y = x^2$, then $y^3 = yy^2 = x^2x^4 = x^{-1}x^4 = x^3 = e$, showing that the inverse of y is its square as well. Therefore, any time we find a non-identity element of x with the property that $x^3 = e$, we also find that $x^{-1} \neq x$ also has this property. It follows that the number of non-identity elements with this property is even, so that the total number with this property is always odd.

The number of group elements that are not their own inverse is even, because an element and its inverse are inverses of one another, so they always come in pairs.

Problem 33

Prove that if G is a group with the property that the square of every element is the identity, then G is Abelian.

Every element is its own inverse. Therefore,

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba.$$

Problem 35

Prove the assertion made in Example 19 that the set $\{1, 2, \ldots, n-1\}$ is a group under multiplication modulo n if and only if n is prime.

It has been shown in the text that $U(n)$ is a group for all $n > 1$. It suffices to show that $\{1, 2, \ldots, n-1\} = U(n)$ in the case that n is prime. To see this, simply notice that when n is prime, all integers in $\{1, 2, \ldots, n-1\}$ are coprime with n.