Chapter 6 Exercises
Gallian's Book on Abstract Algebra

Spencer T. Parkin

February 14, 2014

Problem 1

Find an isomorphism from the group of integers under addition to the group of even integers under addition.

Let $\phi(x) = 2x$. Then, if $y \in \mathbb{Z}$ is even, then $\phi(y/2) = y$, showing that ϕ is onto. Now for any pair of integers $x, y \in \mathbb{Z}$, if $\phi(x) = \phi(y)$, then $2x = 2y \implies x = y$, showing that ϕ is one-to-one. Now notice that, for any $x, y \in \mathbb{Z}$, we have $\phi(x+y) = 2(x+y) = 2x + 2y = \phi(x) + \phi(y)$, showing that ϕ is operation preserving.

Problem 2

Find $\text{Aut}(\mathbb{Z})$.

Notice that $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$, and that 1 and -1 are the only generators of $\mathbb{Z}$. Therefore, if $\phi \in \text{Aut}(\mathbb{Z})$, then $\phi(1) = 1$ or $\phi(1) = -1$. We now show that there is one and only one automorphism of $\mathbb{Z}$ for each of these cases.

Supposing $\phi(1) = 1$, notice that we must have $\phi(-1) = -1$, since

$$0 = \phi(0) = \phi(1 + -1) = \phi(1) + \phi(-1) = 1 + \phi(-1).$$

Then, for any $z \in \mathbb{Z}$, we have

$$\begin{aligned}\phi(z) &= \phi\left(\frac{z}{|z|}(\underbrace{1+\cdots+1}_{|z|})\right) \\ &= \underbrace{\phi\left(\frac{z}{|z|}\right)+\cdots+\phi\left(\frac{z}{|z|}\right)}_{|z|} \\ &= \underbrace{\frac{z}{|z|}+\cdots+\frac{z}{|z|}}_{|z|} = z,\end{aligned}$$

which completely determines ϕ as the identity function.

Now suppose that $\phi(1) = -1$. We then have $\phi(-1) = 1$, since

$$0 = \phi(0) = \phi(1+-1) = \phi(1) + \phi(-1) = -1 + \phi(-1).$$

Then, for any $z \in \mathbb{Z}$, we have

$$\begin{aligned}\phi(z) &= \phi\left(\frac{z}{|z|}\underbrace{(1+\cdots+1)}_{|z|}\right) \\ &= \underbrace{\phi\left(\frac{z}{|z|}\right)+\cdots+\phi\left(\frac{z}{|z|}\right)}_{|z|} \\ &= \underbrace{\frac{-z}{|z|}+\cdots+\frac{-z}{|z|}}_{|z|} = -z,\end{aligned}$$

which completely determines ϕ.

We now see that $\mathrm{Aut}(\mathbb{Z}) = \{z \to z, z \to -z\}$.

Problem 4

Show that $U(8) \not\approx U(10)$.

Notice that $U(8)$ is not cyclic while $U(10) = \langle 3 \rangle$.

Problem 5

Show that $U(8) \approx U(12)$.

This follows from an examination of the Caylay tables for each. Is there a better way?

Problem 6

Prove that the notion of group isomorphism is transitive. That is, if G, H, and K are groups and $G \approx H$ and $H \approx K$, then $G \approx K$.

Let α be an isomorphism between G and H, and β be an isomorphism between H and K. Clearly $\alpha\beta$ is a bijection between G and K. That it is operation preserving follows, for all $a, b \in G$, from

$$(\alpha\beta)(ab) = \alpha(\beta(ab)) = \alpha(\beta(a)\beta(b)) = \alpha(\beta(a))\alpha(\beta(b)) = (\alpha\beta)(a)(\alpha\beta)(b).$$

Problem 9

In the notation of Theorem 6.1, prove that T_e is the identity and that $(T_g)^{-1} = T_{g^{-1}}$.

$$T_e(T_g(x)) = T_e(gx) = egx = gx = T_g(x)$$

Similarly, $T_g(T_e(x)) = T_g(x)$. We then see that

$$T_g(T_{g^{-1}}(x)) = T_g(g^{-1}x) = gg^{-1}x = x = T_e(x).$$

Similarly, $T_{g^{-1}}(T_g(x)) = T_e(x)$.

Problem 10

Let G be a group. Prove that the mapping $\alpha(g) = g^{-1}$ for all $g \in G$ is an automorphism if and only if G is Abelian.

Suppose $\phi \in \mathrm{Aut}(G)$. Then for all $a, b \in G$, we have

$$ab = \phi(a^{-1})\phi(b^{-1}) = \phi(a^{-1}b^{-1}) = \phi((ba)^{-1}) = ba,$$

showing that G is Abelian.

Now suppose that G is Abelian. Let $a, b \in G$ such that $\phi(a) = \phi(b)$. Then $a^{-1} = b^{-1} \implies a = b$, so ϕ is one-to-one. If $a \in G$, then $\phi(a^{-1}) = a$, showing that ϕ is onto. Then, for any $a, b \in G$, we have

$$\phi(ab) = (ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} = \phi(a)\phi(b),$$

by the Abelian property of G, showing that ϕ is operation preserving.

Problem 15

If G is a group, prove that $\mathrm{Aut}(G)$ and $\mathrm{Inn}(G)$ are groups.

It is clear that the identity function ϵ is in $\mathrm{Aut}(G)$. Let $\alpha, \beta \in \mathrm{Aut}(G)$. Notice that if each of α and β are bijections from G to G, then so is $\alpha\beta$. Letting $a, b \in G$, we see that

$$\alpha(\beta(ab)) = \alpha(\beta(a)\beta(b)) = \alpha(\beta(a))\alpha(\beta(b)),$$

showing that $\alpha\beta$ is operation preserving as well. Thus far we have proven closure. Now notice that if α is a bijection of G, then so is α^{-1}. To show that α^{-1} is operation preserving, notice that

$$\alpha(\alpha^{-1}(a)\alpha^{-1}(b)) = \alpha(\alpha^{-1}(a))\alpha(\alpha^{-1}(b)) = ab = \alpha(\alpha^{-1}(ab)),$$

and then take the α^{-1} of both of the furthest sides of this equation. We now see that if $\alpha \in \mathrm{Aut}(G)$, then so is α^{-1}. Notice that function composition is always associative. We can now clame that $\mathrm{Aut}(G)$ is a group.

To show that $\mathrm{Inn}(G)$ is a subgroup of $\mathrm{Aut}(G)$, we first note that it is a subset of $\mathrm{Aut}(G)$, then use the two-step subgroup test. Notice that $\epsilon \in \mathrm{Inn}(G)$, since $\epsilon(g) = ege^{-1} = g$. Let $\alpha, \beta \in \mathrm{Inn}(G)$. Clearly $\alpha\beta \in \mathrm{Inn}(G)$, since, for some $x, y \in G$, we have $\alpha(g) = xgx^{-1}$, $\beta(g) = ygy^{-1}$ and $\alpha(\beta(g)) = x(ygy^{-1})x^{-1} = xyg(xy)^{-1}$ with $xy \in G$. Now notice that $\alpha^{-1}(g) = x^{-1}gx$, but if we let $y = x^{-1}$, it is clear that $\alpha^{-1} \in \mathrm{Inn}(G)$ also.

Problem 17

Let $r \in U(n)$. Prove that the mapping $\alpha : Z_n \to Z_n$ defined by $\alpha(s) = sr \pmod{n}$ for all $s \in Z_n$ is an automorphism of Z_n.

It is clear that α is onto, because $\langle r \rangle = Z_n$ since $\gcd(r, n) = 1$. Then, since α maps a finite set to another of the same cardinality, it is also one-to-one. To see that α is operation preserving, we write, for any $a, b \in Z_n$,

$$\alpha(a + b) = s(a + b) = sa + sb = \alpha(a) + \alpha(b).$$

This proof was nothing more than a generalization of what was given in Example 13.

Problem 19

Prove Property 3 of Theorem 6.3.

If $G \approx \overline{G}$, then there is no loss in generality if we let $G = \overline{G}$.

It was shown in Problem 15 that $\text{Aut}(G)$ is a group. Therefore, if $\phi \in \text{Aut}(G)$, so is ϕ^{-1}.

Problem 20

Prove Property 4 of Theorem 6.3.

We want to show that if K is a subgruop of G, and ϕ is an isomorphism from G to $\overline{G}$, then $\phi(K) = \{\phi(k) | k \in K\}$ is a subgroup of $\overline{G}$.

Clearly $\phi(K)$ is a non-empty subset of $\overline{G}$. Then, for any $a, b \in \overline{G}$, let $x, y \in G$ such that $\phi(x) = a$ and $\phi(y) = b$, and see that

$$ab^{-1} = \phi(x)(\phi(y))^{-1} = \phi(x)\phi(y^{-1}) = \phi(xy^{-1}) \in \overline{G},$$

since $xy^{-1} \in G$ and by Property 2 of Theorem 6.2. It follows that $\phi(K)$ is a subgroup of $\overline{G}$ by the one-step subgroup test.

Problem 21

Referring to Theorem 6.1, prove that T_g is indeed a permutation on the set G.

This simply follows from that fact that the Caylay table for any group must be a Latin square. Notice that $\{T_g(x) | x \in G\}$ is simply one row of this table, and that no element can be repeated in this row if it is a Latin square. (Proof that Caylay tables are Latin squares was given in the solution to a previous chapter's exercise.)

Problem 29

Consider the following statement: The order of a subgroup divides the order of the group. Suppose you could prove this for finite permutation groups. Would the statement then be true for all finite groups? Explain.

Yes. For any finite group in question, Caylay's Theorem tells us that there is a group of permutations isomorphic to it. Therefore, all algebraic and group theoretic properties of this permutation group are shared by the original the group in question.

The whole of group theory may be reduced to the theory of permutation groups.

Problem 30

Suppose that G is a finite Abelian group and G has no element of order 2. Show that the mapping $g \to g^2$ is an automorphism of G. Show, by example, that if G is infinite the mapping need not be an automorphism.

Notice that the only element $g \in G$ with the property that $g^2 = e$ is e itself. Now suppose we have $a, b \in G$ with $\phi(a) = \phi(b)$ and $\phi(g) = g^2$, and notice that $a^2 = b^2 \implies a^2b^{-2} = e \implies (ab^{-1})^2 = e$ by the Abelian property of G. It then follows that $ab^{-1} = e \implies a = b$, and that ϕ is one-to-one. Then, since ϕ is one-to-one and maps a finite set to another, it must also be onto. Now notice that for any $a, b \in G$, we have

$$\phi(ab) = (ab)^2 = a^2b^2 = \phi(a)\phi(b),$$

by the Abelian property of G, showing that ϕ is operation preserving.

Now consider $\mathbb{Z}$, the set of integers, under the addition operation. Notice that $(-1)^2 = 1^2$, but $-1 \neq 1$.

Problem 31

Let G be a group and let $g \in G$. If $z \in Z(G)$, show that the inner automorphism induced by g is the same as the inner automorphism induced by zg (that is, that the mappings ϕ_g and ϕ_{zg} are equal).

Simply notice that

$$\phi_{zg}(x) = zgx(zg)^{-1} = zgxg^{-1}z^{-1} = gxg^{-1}zz^{-1} = gxg^{-1} = \phi_g(x),$$

since z commutes with all elements of G.

Problem 33

Suppose that g and h induce the same inner automorphism of a group G. Prove that $h^{-1}g \in Z(G)$.

Since $\phi_g = \phi_h$, we have, for all $x \in G$,

$$gxg^{-1} = hxh^{-1} \iff h^{-1}gx = xh^{-1}g,$$

showing that $h^{-1}g$ commutes with all elements in G, and therefore, $h^{-1}g \in Z(G)$.

Problem 34

Combine the results of Exercises 31 and 33 into a single "if and only if " theorem.

The converse of the statement proved in Exercise 33 is clearly true by the proof given in that exercise. So we have $h^{-1}g \in Z(G) \iff \phi_h = \phi_g$. It is not clear to me how Problem 31 contributes to this result.

Interestingly, this shows that all members of the center of a group induce the same automorphism of the group.

Problem 35

Let a belong to a group G and let $|a|$ be finite. Let ϕ_a be the automorphism of G given by $\phi_a(x) = axa^{-1}$. Show that $|\phi_a|$ divides $|a|$. Exhibit an element a from a group for which $1 < |\phi_a| < |a|$.

Notice that for a positive integer k, we have

$$\phi_a^k(x) = a^k x(a^{-1})^k = a^k x(a^k)^{-1}.$$

From this it is clear that $\phi^{|a|}(x)$ is the identity automorphism in $\mathrm{Aut}(G)$. Then, by Corollary 2 of Theorem 4.1, we see that $|\phi_a|$ divides $|a|$.

I'm failing to find an example so far.

Problem 40

Show that every automorphism of ϕ of the rational numbers Q under addition to itself has the form $\phi(x) = x\phi(1)$.

It is clear that $\phi(0) = 0 = 0\phi(0)$. So let $x \in Q$ be any non-zero rational. Then there are integers a and b, with $b > 0$, such that $x = a/b$. We then see that

$$\begin{aligned}\phi\left(\frac{a}{b}\right) &= \phi\left(\frac{a}{|a|}\underbrace{\left(\frac{1}{b} + \cdots + \frac{1}{b}\right)}_{|a|}\right) \\ &= \underbrace{\phi\left(\frac{a}{|a|b}\right) + \cdots + \phi\left(\frac{1}{|a|b}\right)}_{|a|} \\ &= |a|\phi\left(\frac{a}{|a|b}\right) = \frac{|a|}{b}\phi\left(\frac{a}{|a|}\right) = \frac{a}{b}\phi(1),\end{aligned}$$

by Property 2 of Theorem 6.2, and by

$$\phi\left(\frac{a}{|a|}\right) = \phi\left(\frac{a}{|a|}\underbrace{\left(\frac{1}{b} + \cdots + \frac{1}{b}\right)}_{b}\right) = b\phi\left(\frac{a}{|a|b}\right).$$

A little bit of abuse of notation has to be allowed to get this result. Admittedly, I can't reconcile myself with it completely, but Gallian says to not get bogged down too much in notation.

Problem 42

Prove that Q, the group of rational numbers under addition, is not isomorphic to a proper subgroup of itself.

By the answer to Problem 40, every isomorphism of Q, not just onto itself, but to any other additive group of rational numbers, must be of the form $\phi(x) = x\phi(1)$. It is then clear that $\phi(Q)$, the image of Q under ϕ, must be Q itself, because $\phi(1) \neq 0 = \phi(0)$.

Made-Up Problems

Problem 1

For any geometric algebra $\mathbb{G}$, show that the set of all versors $V \in \mathbb{G}$ forms a group under the geometric product. Does the set of all unit-versors form a subgroup?

The geometric product is associative. Notice that 1 is the identity versor. Let $A, B \in \mathbb{G}$ be versors. There then exists a set of m invertible vectors $\{a_i\}_{i=1}^m$ and a set of n invertible vectors $\{b_i\}_{i=1}^n$ such that $A = \prod_{i=1}^m a_i$ and $B = \prod_{i=1}^n b_i$. It now follows by the definition of what a versor is, that AB is also a versor. AB is a product of one or more invertible vectors. Now notice that $A^{-1} = \prod_{i=1}^m a_{m-i+1}^{-1}$ is also, by definition, a versor. (It may also be required to say that by the zero-product property of the geometric property, inverses are unique.)

Seeing that $|A| = \prod_{i=1}^m |a_i|$, (this is not hard to prove), if $|A| = 1$, we can, without loss of generality, assume, for each a_i, that $|a_i| = 1$. (Such a set of m vectors can always be found for A.) Do the same for B. Closure then follows. Note that the identity has magnitude 1. Then, seeing that, for any a_i, we have $|a_i| = |a_i^{-1}|$, we also have inverses. So the unit-versors form a subgroup of the versor group.

Problem 2

Show that the even versors of a geometric algebra $\mathbb{G}$ form a group under the geometric product? Do the odd versors form a group?

Clearly the odd versors don't form a group, because we don't have closure. The even versors give us closure. The identity versor may be considered even. And it is clear the the inverse of an even versor is also even.

Problem 3

For a geometric algebra $\mathbb{G}$, show that the function $\phi_W(V) = WVW^{-1}$, with W a versor of $\mathbb{G}$, is an automorphism of the group of versors of $\mathbb{G}$.

Let A and B be versors such that $\phi_W(A) = \phi_W(B)$. Then $WAW^{-1} = WBW^{-1}$ implies that $A = B$ trivially, and ϕ_W is one-to-one. Now let B be any versor and let $A = W^{-1}BW$ and notice that $\phi(A) = B$, showing that ϕ_W is onto. That ϕ_W is operator preserving follows from, for any versors A

and B,

$$\phi_W(AB) = WABW^{-1} = WAW^{-1}WBW^{-1} = \phi_W(A)\phi_W(B).$$

Problem 4

For a geometric algebra $\mathbb{G}$ and a fixed positive integer k, show that the k-vectors of $\mathbb{G}$ form a group under addition. Do the k-blades form a group? (Let zero be a k-vector for any k.)

k-blades don't generally form a group, because we don't always have closure for $k \geq 2$. (In some geometric algebras, we do have closure for $k = 2$, but not all.)

k-vectors do give us closure. Zero is the zero k-vector. k-vector addition is associative. The additive inverse of a k-vector is easy to calculate and it is unique.

Problem 5

For any versor W in a geometric algebra $\mathbb{G}$, define the function $\phi_W(V) = WVW^{-1}$ on the set of k-vectors in $\mathbb{G}$, and show that it is an automorphism of the group of k-vectors.

We begin by showing that the set of k-vectors is closed under the operation of conjugation by any versor W. By induction, we need only consider the case when W is a vector. First note that, by the linearity of the operation, it is sufficient to show closure in the set of all k-blades under this operation. Letting A be a vector, it is easy to verify that WAW^{-1} is a vector. Letting A be a k-blade with factorization $A = \bigwedge_{i=1}^{k} a_i$, and seeing that, by the outermorphic property of conjugation by versors, we have

$$WAW^{-1} = \bigwedge_{i=1}^{k} Wa_iW^{-1},$$

it follows that WAW^{-1} is a k-blade also.

Returning to the problem at hand, let A and B be k-vectors such that $\phi_W(A) = \phi_W(B)$. Then $WAW^{-1} = WBW^{-1}$ implies that $A = B$. Now let B be any k-vector and let $A = W^{-1}BW$ be a k-vector too. It follows that $\phi_W(A) = B$. Now let A and B be any two k-vectors and notice that

$$\phi_W(A + B) = W(A + B)W^{-1} = WAW^{-1} + WBW^{-1} = \phi_W(A) + \phi_W(B).$$