Chapter 3 Exercises
Gallian's Book on Abstract Algebra

Spencer T. Parkin

January 31, 2014

Problem 3

Let Q and Q^* be as in Exercise 2. Find the order of each element of Q and Q^*.

For a given $q \in Q$, let $a, b \in \mathbb{Z}$ be integers, with $b \neq 0$, such that $q = a/b$. We seek the smallest positive integer n for which $nq = na/b = 0$. If $a = 0$, then $n = 1$. If $a \neq 0$, then there is no such integer. The order of non-identity elements in Q is therefore infinite.

For a given $q \in Q^*$, let $a, b \in \mathbb{Z}$ be integers, with $b > 0$, such that $q = a/b$. We seek the smallest positive integer n for which $q^n = a^n/b^n = 1$. If $a = b$, then $q = 1$ and $n = 1$. If $|a| < b$, then for all $n > 1$, we have $|a^n/b^n| < a/b < 1$, showing that the order of q, in this case, is infinite. If $|a| > b$, then for all $n > 1$, we have $|a^n/b^n| > a/b > 1$, show that the order of q, also in this case, is infinite.

(Check this one.)

Problem 4

Prove that in any group, an element and its inverse have the same order.

Let G be a group and let a be an element of G. Now notice that

$$(a^{-1})^{|a|} = (a^{|a|})^{-1} = e^{-1} = e.$$

Problem 5

Without actually computing the orders, explain why the two elements in each of the following pairs of elements from Z_{30} must have the same order: $\{2, 28\}$, $\{8, 22\}$. Do the same for the following pairs of elements from $U(15)$: $\{2, 8\}$, $\{7, 13\}$.

In the first two cases, notice that the pairs of numbers are congruent modulo 30. Therefore, their additive powers are congruent modulo 30, so they have the same order.

In the second two cases, notice that the pairs of numbers are inverses of one another. So by Problem 4 above, they must have equal order.

Problem 6

Let x belong to a group. If $x^2 \neq e$ and $x^6 = e$, prove that $x^4 \neq e$ and $x^5 \neq e$. What can we say about the order of x?

Supposing $x^4 = e$, we see that $e = x^6 = x^4x^2 = x^2$, which is a contradiction. Therefore, $x^4 \neq e$. Supposing $x^5 = e$, we see that $e = x^6 = x^5x = x \implies x^2 = e$, which reaches the same contradiction. Therefore, $x^5 \neq e$.

It is clear that $x \neq e$. Supposing $x^3 = e$, we do no contradict any of the facts uncovered so far. So the order of x is either 3 or 6.

(Check this one if possible.)

Problem 7

Show that if a is an element of a group G, then $|a| \leq |G|$.

Clearly this is true in the case that $a = e$. Supposing that $a \neq e$, we must have $|a| > 1$.

Now notice that $\{a^i\}_{i=1}^{|a|}$ is a set $|a|$ elements, since for all $1 \leq i < j \leq |a|$, we have $a^i \neq a^j$. To verify this claim, suppose $a^i = a^j$. Then $a^{j-i} = e$, but $j - i < |a|$, which is a contradiction.

We can now say that if $|a| > |G|$, then G is a proper subset of $\langle a \rangle$, but this violates the closure of the product under G.

Problem 8

Show that $U(14) = \langle 3 \rangle = \langle 5 \rangle$. [Hence, $U(15)$ is cyclic.] Is $U(14) = \langle 11 \rangle$?

After manually verifying that $U(14) = \langle 3 \rangle$, we can easily show that $\langle 5 \rangle = \langle 3 \rangle$ by noting that $5^i \equiv 3^{5i} \pmod{14}$ and that 5 generates the additive cyclic group Z_6, since $1 = \gcd(5, 6)$.

(How was it proven again that $k \in Z_n$ generates Z_n if $1 = \gcd(k, n)$?)

Problem 9

Show that $U(20) \neq \langle k \rangle$ for any k in $U(20)$. [Hence, $U(20)$ is not cyclic.]

By inspection, there is no element of order $|U(20)|$. I'm sure there's a theorem that would make it easier to come to this conclusion.

Problem 10

Prove that an Abelian group with two elements of order 2 must have a subgroup of order 4.

Let a and b be two elements of this group having order 2. Clearly the elements in the set $\{e, a, b, ab\}$ are in the group. We now show that it is a sub-group. Closure in this set is trivial for all but the following cases. Note that $a^2 = b^2 = e$ is in the set. Note that $ba = ab$ is in the set, as well as $aab = b$, $aba = b$, $bab = a$ and $abb = a$, and finally, $abab = aabb = e$ is in the set. Now notice that $e^{-1} = e$, $a^{-1} = a$, $b^{-1} = b$ and $(ab)^{-1} = b^{-1}a^{-1} = ab$. It follows that $\{e, a, b, ab\}$ is a subgroup by Theorem 3.2.

Problem 13

For each divisor $k > 1$ of n, let $U_k(n) = \{x \in U(n) | x \equiv 1 \pmod{k}\}$. Prove that $U_k(n)$ is a subgroup of $U(n)$.

It is clear that $1 \in U_k(n)$, so it is not empty; and it is clear that $U_k(n)$ is a subset of $U(n)$. Closure is obvious. By Theorem 3.2, what then remains to be shown is that for any $a \in U_k(n)$, we have $a^{-1} \in U_k(n)$. To that end, notice that since $k|n$ and $n|(aa^{-1} - 1)$, we have $k|(aa^{-1} - 1)$. Then since $a \equiv 1 \pmod{k}$ and $aa^{-1} \equiv 1 \pmod{k}$, we must have $a^{-1} \equiv 1 \pmod{k}$.

Problem 14

If H and K are subroups of G, show that $H \cap K$ is a subgroup of G.

Note that $e \in H \cap K$, so it is non-empty. Letting $a, b \in H \cap K \subseteq G$, we see, by Theorem 3.1, that since $a, b \in H$, we have $ab^{-1} \in H$, and since $a, b \in K$, we have $ab^{-1} \in K$. It follows that $ab^{-1} \in H \cap K$ and that, by Theorem 3.1 again, $H \cap K$ is a subgroup of G.

Using induction, it can be shown that the intersection of all sub-groups in any sequence of subgroups is itself a subgroup. What about the intersection of uncountably many subgroups?

Let S be an uncountably infinite collection of subgroups of G. Consider the set $H = \cap_{g \in S} g$. Letting $a, b \in H$, we have, for all $g \in S$, $ab^{-1} \in g$, and therefore, $ab^{-1} \in H$. It follows that H is also a subgroup of G.

Could we form some sort of topology from this idea?

Problem 15

Let G be a group. Show that $Z(G) = \cap_{a \in G} C(a)$.

It is clear that $\cap_{a \in G} C(a)$ is a group by Problem 14 above, since each $C(a)$ is a sub-group of G. Now notice that $x \in \cap_{a \in G} C(a)$ if and only if x communites with every a in G. But this is the very defining characteristic of all elements in $Z(G)$. So these sets are the same set.

Problem 16

Let G be a group, and let $a \in G$. Prove that $C(a) = C(a^{-1})$.

Notice that since $(a^{-1})^{-1} = a$, we need only show that $C(a) \subseteq C(a^{-1})$. Now see that if $x \in C(a)$, then $xa = ax$, which, in turn, implies that $x = axa^{-1}$, which implies that $a^{-1}x = xa^{-1}$, showing that $x \in C(a^{-1})$ also.

Problem 18

If a and b are distinct group elements, prove that either $a^2 \neq b^2$ or $a^3 \neq b^3$.

If $a^2 \neq b^2$, then we're done. If $a^2 = b^2$, then suppose $a^3 = b^3$. It follows that $b^2 b = b^3 = a^3 = a^2 a = b^2 a \implies a = b$, which is a contradiction, because a and b are distinct elements. It follows that $a^3 \neq b^3$.

Problem 19

Prove Theorem 3.6. For each a in a group G, the centralizer of a is a subgroup of G.

Notice that $e \in C(a)$, since $ea = a = ae$, so $C(a)$ is non-empty. (We could have also shown that $a \in C(a)$.) Let $x, y \in C(a)$. Then $ax = xa \implies axy = xay = xya \implies xy \in C(a)$, and $a = x^{-1}xa = x^{-1}ax \implies ax^{-1} = x^{-1}a \implies x^{-1} \in C(a)$. So $C(a)$ is a subgroup by Theorem 3.2.

Problem 20

If H is a subgroup of G, then by the centralizer $C(H)$ of H we mean the set $\{x \in G | xh = hx \text{ for all } h \in H\}$. Prove that $C(H)$ is a subgroup of G.

If I'm not mistaken, H need not be a subgroup of G. By Problem 14, $C(H) = \cap_{h \in H} C(h)$ is a subgroup of G.

Problem 21

Must the centralizer of an element of a group be Abelian?

No. Let G be a non-Abelian group. Now notice that $C(e) = G$ is non-Abelian. A harder question is: For some non-identity element $a \in G$ with G non-Abelian, can $C(a)$ be non-Abelian? I have yet to find an example, but do not discount the possibility.

Problem 22

Must the center of a group be Abelian?

Yes. Every element of $Z(G)$ commutes with all elements of G, which includes all those of $Z(G)$.