Chapter 4 Exercises
Gallian's Book on Abstract Algebra

Spencer T. Parkin

February 6, 2014

Problem 11

Let G be a group and let $a \in G$. Prove that $\langle a^{-1} \rangle = \langle a \rangle$.

Suppose a has finite order n. Then $a^{-1} = a^{n-1}$ and since $\gcd(n, n-1) = 1$, it follows that $\langle a^{-1} \rangle = \langle a^{n-1} \rangle = \langle a^{\gcd(n,n-1)} \rangle = \langle a \rangle$.

Suppose now that a has infinite order. In this case, it is clear that

$$\langle a^{-1} \rangle = \{a^{-k} | k \in \mathbb{Z}\} = \{a^k | k \in \mathbb{Z}\} = \langle a \rangle.$$

Problem 12

Suppose that a has infinite order. Find all generators of the subgroup $\langle a^3 \rangle$.

All members of this group have the form a^{3k} for some integer k. A generator of this group, therefore, has such a form. The only possible generators must be elements a^{3k} for $k = 1$ or $k = -1$.

Problem 13

Suppose that $|a| = 24$. Find a generator for $\langle a^{21} \rangle \cap \langle a^{10} \rangle$. In general, what is a generator for the subgroup $\langle a^m \rangle \cap \langle a^n \rangle$?

It is clear that

$$\langle a^m \rangle \cap \langle a^n \rangle = \{(a^{\text{lcm}(m,n)})^k | k \in \mathbb{Z}\}.$$

Therefore, a^s, with $s = \text{lcm}(m, n)$ is a generator. We can also let $s = \text{lcm}(m, n) \mod |a|$. Doing so, we have

$$\langle a^{21} \rangle \cap \langle a^{10} \rangle = \langle a^2 \rangle.$$

Problem 14

Suppose that a cyclic group G has exactly three subgroups: G itself, $\{e\}$, and a subgroup of order 7. What is $|G|$? What can you say if 7 is replaced with p where p is prime?

According to Theorem 4.3, if $G = \langle a \rangle$, then, for every positive divisor z of $|G|$, we have

$$|\langle a^{|G|/z} \rangle| = z,$$

and exactly one subgroup of that order. If there are exactly three distinct subgroups of G, then there are exactly three distinct and positive divisors of $|G|$, namely $1 < p < |G|$. It follows that $|G| = p^2$.

Problem 15

Let G be an Abelian group and let $H = \{g \in G | |g| \text{ divides } 12\}$. Prove that H is a subgroup of G. Is there anything special about 12 here? Would your proof be valid if 12 were replaced by some other positive integer. State the general result.

For any positive integer z, let $H = \{g \in G | |g| \text{ divides } z\}$, where G is an Abelian group. Then H is a subgroup of G.

Note that $e \in H$. Then, for any $a, b \in H$, we must show that $|ab^{-1}|$ divides z. Since G is Abelian, we see that $(ab^{-1})^k = a^k(b^k)^{-1}$, and so $|ab^{-1}| = \text{lcm}(|a|, |b|)$. It now follows that since $|a|$ divides z and $|b|$ divides z, we have $\text{lcm}(|a|, |b|)$ dividing z as well. (An argument for this can be made by considering prime factorizations.)

Problem 20

Suppose that G is an Abelian group of order 35 and every element of G satisfies the equation $x^{35} = e$. Prove that G is cyclic. Does your argument work if 35 is replaced with 33?

It is clear that the only possible orders of elements in G are 1, 5, 7 and 35. There is only ever 1 element of order 1; namely, the identity. If there is an element of order 35, we're done. So suppose there's an element of order 5. Then, by the Corollary to Theorem 4.4, there can at most be some multiple of $\phi(5)$ elements of this order. But $\phi(5) = 4$ does not divide $35 - 1 = 34$, so there must also exist an element of order 7 or 35. If there is an element of order 35, we're done, so let there exist an element of order 7. Let $x, y \in G$ be elements of orders 5 and 7, respectively. Now notice that $|xy| = \text{lcm}(5, 7) = 35$, because $(xy)^k = x^k y^k$ by the Abelian property of G.

Now suppose that there's an element of order 7. Then there can at most be some multiple of $\phi(7)$ of these, but $\phi(7) = 6$ also does not divide 34. So there must be an element of order 5 or 35. Assuming it's not 35, we can again let $x, y \in G$ be elements of orders 5 and 7, respectively, and see that $|xy| = 35$.

Now since in all cases, we can show that an element of order 35 exists in G, and the order of G is 35, we can conclude that G is a cyclic group.

Replacing 35 with 33, this argument fails, because the possible orders are 1, 3, 11 and 33, and $\phi(3) = 2$ does divide $33 - 1 = 32$.

Problem 22

Prove that a group of order 3 must be cyclic.

This is easily shown by considering the Caylay table.

	e	a	b
e	e	a	b
a	a	a^2	ab
b	b	ba	b^2

It is clear here that the only choice for $ab = e$, and the only choice for $ba = e$. It follows that $a^2 = b$ and $b^2 = a$. We can now see that a or b generates the group.

Problem 23

Let Z denote the group of integers under addition. Is every subgroup of Z cyclic? Why? Describe all the subgroups of Z.

Let $G < Z$, and let $a \in G$ be an element with the smallest possible absolute value. (Such an element exists by the well-ordering principle.) Now consider the cyclic subgroup $\langle a \rangle \leq G$. Supposing this to be a proper subgroup, let $x \in G - \langle a \rangle$. But now since a does not divide x, there exists an integer k such that $\text{abs}(x + ka) < \text{abs}(a)$, which is a contradiction. It follows that $\langle a \rangle = G$.

The subgroups of Z are all of the form $\langle a \rangle$ for some $a \in G$.

Problem 24

For any element a in any group G, prove that $\langle a \rangle$ is a subgroup of $C(a)$.

Since each of these are subgroups of G, it sufficies to show that $\langle a \rangle$ is a subset of $C(a)$. Letting $x \in \langle a \rangle$, there exists $k \in \mathbb{Z}$ such that $x = a^k$. Now notice that $ax = aa^k = a^{k+1} = a^k a = xa$, showing that x communites with a, and therefore, $x \in C(a)$.

Problem 42

Prove that an infinite group must have an infinite number of sugroups.

Notice that such a group must have an element x of infinite order. Now consider the cyclic subgroup $\langle x \rangle$, and realize that it has an infinite number of subgroups, because Z has an infinite number of subgroups.

Problem 43

Let p be prime. If a group has more than $p - 1$ elements of order p, why can't the group be cyclic?

Suppose we have a finite group of order n. If it has an element of order p, then p must be a divisor of n. Furthermore, there is exactly one cyclic subgroup of order p. Let x be an element of order p. Now see that all elements in $\langle x \rangle$ must have order p, because all positive integers less than p are coprime with p. So $\langle x \rangle$ contains $p - 1$ elements of order p. If the group has more than $p - 1$ elements of order p, then let $y \notin \langle x \rangle$ be an element of order p, and notice that $\langle x \rangle \cap \langle y \rangle = \emptyset$, showing that there are at least $2(p-1)$ elements of order p in the group. The group is therefore not cyclic, because there must be exactly one cyclic subgroup of order p.

Supposing now that we have an infinite group, it is easy how the same type of argument applies.

Problem 56

Prove that $U(2^n)$ $(n \geq 3)$ is not cyclic.

For any set of integers S, letting $-S$ denote the set $\{-s|s \in S\}$, we first make the observation that

$$U(2^n) = U(2^{n-1}) \cup -U(2^{n-1}),$$

working modulo 2^n. (Notice that $U(2^{n-1})$ is not a subgroup of $U(2^n)$, because it does not share its group operation with $U(2^n)$.) Now notice that since $|U(2^n)| = 2^{n-1}$ is even, all orders of elements in $U(2^n)$ are even, and therefore, the order of any element $x \in -U(2^{n-1})$ is that of its corresponding element $-x \in U(2^{n-1})$. It follows that if no generator for $U(2^n)$ can be found in $U(2^{n-1})$, then no generator for it can be found in $-U(2^{n-1})$.

We now proceed by induction. The case $n = 3$ is easily verifiable. Suppose now that for a fixed integer $n > 3$, we have $U(2^{n-1})$ non-cyclic. We must show that $U(2^n)$ is non-cyclic. To that end, notice that if $U(2^{n-1})$ is non-cyclic, then for every integer k and any element $x \in U(2^{n-1})$, there exists an element $y \in U(2^{n-1})$ such that 2^{n-1} does not divide $x^k - y$. In all such situations, we can also say that 2^n does not divide $x^k - y$ either. It follows that there is no generator for $U(2^n)$ in $U(2^{n-1})$, and therefore, by the first paragraph of this proof, $U(2^n)$ is also non-cyclic. We can now say, by the principle of mathematical induction, that $U(2^n)$ is non-cyclic for all $n \geq 3$.