Section 2.5 Exercises
Hertein's Topics In Algebra

Spencer T. Parkin

March 4, 2016

Understanding Theorem 2.5.1

Here, a leap was made for me in realizing that for every $h_1, h_2 \in H \cap K$, we have $hh_1 \neq hh_2$ and $h_1^{-1}k \neq h_2^{-1}k$. This is obvious by the cancelation proprety. So what he does is show that $o(H \cap K)$ duplicates of the element hk exists in the $o(HK)$ possible multiplications of an element taken from H with that of K. He then shows that this lower bound is also an upper bound, and the rest goes through.

Problem 1

If H and K are subgroups of G, show that $H \cap K$ is a subgroup of G. (Can you see that the same proof shows that the intersection of any number of subgroups of G, finite or infinite, is again a subgroup of G?)

Let's just go ahead and show the result for an arbitrary intersection. Let I be an index set for a family of subgroups H_α of G. Is $H = \bigcap_{\alpha \in I} H_\alpha$ a subgroup of G?

Clearly $e \in H$, since all subgroups contain the identity element; so H is non-empty. Now for all $a, b \in H$, and for any $\alpha \in I$, notice that $a \in H \subseteq H_\alpha$ and $b \in H \subseteq H_\alpha$, so $ab \in H_\alpha$. It follows that $ab \in H$. Now since for all $a \in H$, and all $\alpha \in I$, we have $a \in H \subseteq H_\alpha$, we have $a^{-1} \in H_\alpha$; and therefore, $a^{-1} \in H$. That H is a subgroup of G now follows by Lemma 2.4.1.

Problem 2

Let G be a group such that the intersection of all its subgroups which are different from $\langle e \rangle$ is a subgroup different form $\langle e \rangle$. Prove that every element in G has finite order.

We show the contrapositive. Let $a \in G$ be an element of infinite order. We must now show that the intersection of all subgroups, save $\{e\}$, is the trivial subgroup $\{e\}$. But this is easy. We need only show that this is the case for the subgroup generated by a; namely, $\langle a \rangle$. Being isomorphic to the integers, let us just consider $\mathbb{Z}$. Notice that for any integer $n > 0$, $\mathbb{Z}$ has a subgroup with smallest positive non-identity element equal to n. It follows that the intersection of all subgroups, save $\{0\}$, is $\{0\}$.

Problem 3

If G has no nontrivial subgroups, show that G must be finite of prime order.

We first show that G is finite by showing that every infinite group has at least one nontrivial subgroup. If an infinite group has no nontrivial subgroups, then every non-identity element would generate the entire group. But this is impossible, because every non-identity element of infinite order generates $\mathbb{Z}$, which has non-trivial subgroups.

Now consider $|G|$. If G has a non-trivial subgroup H, then $|H|$ divides $|G|$ and $1 < |H| < |G|$ which implies that $|G|$ is composite. This is no help.

Let $a \in G$ be a non-identity element. Clearly we must have $\langle a \rangle = G$. We now show that the converse of Lagrange's theorem holds for cyclic groups.

Consider the group $\mathbb{Z}_n = \{z \in \mathbb{Z} | 0 \leq z < n\}$ endowed with addition mod n. Let d be any divisor of n. We must find a subgroup of order d of $\mathbb{Z}_n$. This is easy when $d = 1$ or $d = n$. Considering d to be a non-trivial divisor, let's look at $\langle n/d \rangle$. The order of this subgroup is the order n/d in Z_n, which is clearly $n/(n/d) = d$. Thus, for every divisor d of n, $\mathbb{Z}_n$ has a subgroup of order d.

Returning to $\langle a \rangle = G$, we can now say that if $|G|$ was composite, then it would have a non-trivial subgroup. We now have our proof by the contrapositive of this statement.

(Note also that all subgroups of a cyclic group are cyclic, and that there is *exactly* one subgroup of order d for every divisor d of $\mathbb{Z}_n$. Proof is needed, though.)

Problem 4

Part (a)

If H is a subgroup of G, and for $a \in G$, $aHa^{-1} = \{aha^{-1} | h \in H\}$, show that aHa^{-1} is a subgroup of G.

Note that $x, y \in aHa^{-1}$ implies that $x = ah_xa^{-1}$ and $y = ah_ya^{-1}$ with $h_x, h_y \in H$. It follows that $xy = ah_xh_ya^{-1} \in aHa^{-1}$ since $h_xh_y \in H$. Then clearly $x^{-1} \in aHa^{-1}$ since $x^{-1} = ah_x^{-1}a^{-1}$. Seeing that $aHa^{-1} \subseteq G$, our proof goes through by Lemma 2.4.1.

Part (b)

If H is finite, what is $|aHa^{-1}|$?

Let $\phi : H \to aHa^{-1}$ be defined as $\phi(x) = axa^{-1}$. Then if $\phi(x) = \phi(y)$, then $axa^{-1} = aya^{-1} \implies x = y$, showing that ϕ is one-to-one. Then since H is finite, ϕ is also onto. It follows that $|H| = |aHa^{-1}|$.

Problem 5

For a subgroup H of G define the left coset aH of H in G as the set of all elements of the form ah, $h \in H$. Show that there is a one-to-one correspondence (bijection) between the set of left cosets of H in G and the set of right cosets of H in G.

The natural mapping to investigate is $\phi(Ha) = aH$ with $a \in G$. Clearly it is onto (surjective). Is it well defined? Is it one-to-one (injective)?

Note that $Hx = Hy$ if and only if $xy^{-1} \in H$. If $xy^{-1} \in H$, then $x \in Hy$. Then since clearly $x \in Hx$, we have $Hx \cap Hy$ non-empty. But now since the right cosets of H in G partition G, we must have $Hx = Hy$. On the other hand, if $Hx = Hy$, then $x \in Hy \implies x \equiv y \pmod{H}$ by Lemma 2.4.4.

It is also possible to show that $x^{-1}y \in H$ if and only if $xH = yH$.

Hmmm...think about it.

Problem 25

Let G be an abelian group and suppose that G has elements of orders m and n, respectively. Prove that G has an element whose order is the least common multiple of m and n.

Find $a, b \in G$ such that $|a| = m$ and $|b| = n$, and then let $x = ab$ and $r = \text{lcm}(m, n)$. We then see that

$$x^r = (ab)^r = a^r b^r = e^2 = e,$$

showing that $|x|$ divides r.

I think we now need to show that $a^k b^k = e$ if and only if $a^k = e$ and $b^k = e$. One direction is trivial...

Problem 27

Prove that any subgroup of a cyclic group is itself a cyclic group.

Let $G = \langle a \rangle$, and let H be a non-trivial subgroup of G. Notice that all elements in H are of the form a^k for some integer k. In other words, $H = \{a^{m_i}\}_i$, where $\{m_i\}_i$ is a set of positive integers. By the well-ordering principle, this set has a smallest element; call it m and consider $a^m \in H$. If $\langle a^m \rangle = H$, then we're done. If not, then $H - \langle a^m \rangle$ is yet another set of elements, each of the form $\{a^{n_i}\}$, where $\{n_i\}_i$ is a set of positive integers. By the well-ordering principle, this set has a smallest element; call it n and consider $a^n \in H - \langle a^m \rangle$. It should be clear that $m < n < 2m$; from which it follows that

$$0 < n - m < m.$$

But now since $a^m, a^n \in H$, we must have

$$e \neq a^n (a^m)^{-1} = a^{n-m} \in H,$$

which is a contradiction of the fact that m is the least positive integer for which $a^m \neq e$. It follows that $H = \langle a^m \rangle$.

Note: Suppose we look at $a^n \in H$ with $km < n < (k+1)m$, where $k > 1$. Then $a^{n-km} \in H$, and $0 < n - km < m$.

Problem 28

How many generators does a cyclic group of order n have?

In $\mathbb{Z}_n$, the number of generators is the number of positive integers less than n and relatively prime to n, denoted $\phi(n)$. How can we prove this? Let

$x \in \mathbb{Z}_n$ be such a number, and choose any $y \in \mathbb{Z}_n$. We want to show that there exists an integer k such that

$$kx \equiv y \pmod{n}.$$

Now since $(x, n) = 1$, there exist integers $u, v \in \mathbb{Z}$ such that

$$ux + vn = 1.$$

Multiplying through by y, we find that

$$(uy)x + (vy)n = y,$$

which shows that $n|(y - kx)$ with $k = uy$.

Thus far we have only shown that the number of generators of $\mathbb{Z}_n$ is at least $\phi(n)$. Are there anymore? Brain farting on how to prove this.