Homework 1

Andrew Tindall
Algebra I

January 22, 2020

Problem 1. (a) Let H and K be subgroups of G. Show that $H \cap K$ is a subgroup, and that $\langle H \cup K \rangle$ is the smallest subgroup containing H and K.

Proof. First, we see that $H \cap K$ is a subgroup: it must contain the identity, because both H and K do, and if elements $x, y \in H \cap K$, then $xy \in H$ and $xy \in K$, by the fact that each is a subgroup. So, $xy \in H \cap K$; and we see that $H \cap K$ is a subgroup.

Now, we show that $\langle H \cup K \rangle$ is the smallest subgroup containing H and K. By definition, $\langle H \cup K \rangle$ is the set of all finite products $x_1 x_2 \cdots x_n$ of elements $x_i \in H \cup K$. This is a group, as it contains the identity element (the product of zero elements), and the product of two elements $x_1 x_2 \cdots x_n$ and $y_1 y_2 \cdots y_m$ is $x_1 x_2 \cdots x_n y_1 \cdots y_m$, which is also a finite product of elements of $H \cup K$.

We can also see that $\langle H \cup K \rangle$ also contains $H \cup K$, as every element $x \in H \cup K$ is a singleton product.

Finally, we want to show that $\langle H \cup K \rangle$ is the smallest subgroup with this properties: that, if $F \leq G$ is a subgroup containing $H \cup K$, then $\langle H \cup K \rangle \leq F$. Let $x \in \langle H \cup K \rangle$. We can write x as a finite product $x_1 \cdots x_n$ of elements of $H \cup K$. Because $H \cup K \subseteq F$, each element x_i is also an element of F, and so is their product x. Since every element of $\langle H \cup K \rangle$ is an element of F, we see that $\langle H \cup K \rangle \leq F$, and so $\langle H \cup K \rangle$ is indeed the smallest group containing both H and K. □

(b) The union of two subgroups is a subgroup if and only if one is included in the other.

Proof. Let H and K be two subgroups of G. One direction is easy: if $H \leq K$, then $H \cup K = K$, which is a subgroup by assumption.

Now, assume that $H \cup K$ is a subgroup of G. We want to show that either $H \leq K$ or $K \leq H$. For sake of contradiction, assume that neither holds: then there are two elements x, y such that $x \in H$ and $x \notin K$; and $y \in K$ and $y \notin H$.

Both x and y are in $H \cup K$, and by the assumption that $H \cup K$ is a subgroup, we know that $xy \in H \cup K$. Either $xy \in H$ or $xy \in K$.

If $xy \in H$, then $x^{-1} \in H$ as well, and so $x^{-1}xy = y \in H$, contradicting our assumption. If $xy \in K$, then $y^{-1} \in K$ as well, and so $xyy^{-1} = x \in K$, contradicting our assumption. We have reached a contradiction, so either $H \leq K$ or $K \leq H$. □

(c) H is a subgroup if and only if $HH = H$.

Proof. H is a subgroup, then $HH \subset H$ by the fact that it is closed under products, and $H \subset HH$ holds by the fact that, for any $x \in H$, the element $ex = x$ is in HH.

In the other direction , if $HH = H$, then H is closed under products, and so we need only check that the identity element e is in H. *incomplete* □

(d) If H and T are subgroups, then $|HT||H \cap T| = |H||T|$.

Proof. If either H or T is infinite, then so is HT, and the equality is $\infty = \infty$. So, assume that $|H|$ and $|T|$ are both less than ∞.

The following proof is from math.stackexchange.com: we want to show that $|HT| = \frac{|H||T|}{|H \cap T|}$. We know that every element of HT can be represented as ht, for some $h \in H$ and $t \in T$, but these h and t may not be unique. We will see that the number of pairs representing each $x \in HT$ is $|H \cap T|$:

For every $ht \in HT$, and $x \in H \cap T$, we see that $hx \in H$ and $x^{-1}t \in T$, so $(hx)(x^{-1}t)$ is another unique way to represent the same element of HT. So there are at least $|H \cap T|$ ways to represent this element.

On the other hand, if $ht = h't'$, then $h^{-1}h' = t't^{-1}$. Setting $x = h^{-1}h' = t't^{-1}$, we see that $x \in H \cap T$, and both $h' = hx$ and $t' = x^{-1}t$, so there are *exactly* $|H \cap T|$ ways to represent any element of HT by pairs of elements of $H \cap T$. So, combinatorially, $|HT| = \frac{|H||T|}{|H \cap T|}$. □

(e) HT is a subgroup if and only if $HT = TH$.

Proof. First, assume that HT is a subgroup. Let $x = th$ be some element of TH. We see that

$$\begin{aligned} x &= th \\ &= (h^{-1}t^{-1})^{-1} \end{aligned}$$

Since $h^{-1}t^{-1} \in HT$, and HT is a subgroup, we see that $(h^{-1}t^{-1})^{-1} = x \in HT$ as well.

In the other direction, if $HT = TH$, we want to show that HT is a subgroup. Since $e = ee \in HT$, we need only show that HT is closed under products. Let $x = h_1t_1$ and $y = h_2t_2$ be two elements of HT. Their product is $h_1t_1h_2t_2$. The element $t_1h_2 \in TH$, so by assumption it must also be in HT; and so $t_1h_2 = h't'$ for some $h' \in H$ and $t' \in T$. So,

$$\begin{aligned} xy &= h_1t_1h_2t_2 \\ &= h_1(h't')t_2 \\ &= (h_1h')(t't_2) \in HT \end{aligned}$$

So, HT is a subgroup. □

(f) If H is a proper subgroup of G, then the set of elements in G but not in H generates G.

Proof. Let $S = G \backslash H$, the set of elements in G but not in H. We want to show that $\langle S \rangle = G$. Since $G = S \cup H$, and $S \subseteq \langle S \rangle$, we only need to show that $H \subset \langle S \rangle$; i.e. that every element of H can be written as a finite product of elements of S.

Let $h \in H$, and pick some $s \in S$. (Some such S must exist because S is nonempty, because H is a proper subset). The element sh cannot be in H, for if it was, then $(sh)(h^{-1}) = s$ would be as well, contradicting the assumption that $s \in S$. Also, the element s^{-1} must be in S, because if $s^{-1} \in H$, then $(s^{-1})^{-1} = s \in H$, again a contradiction. So, the element $h = s^{-1}(sh)$ can be written as a product of elements of S. □

Problem 2. (a) If x has order n, and $n = mk$, then x^k has order m.

Proof. We see that $(x^k)^m = x^{km} = x^n = e$, so the order of x^k is at most m. On the other hand, if the order of $x^k = j$ is less than m, then

$$\begin{aligned} e &= (x^k)^j \\ &= x^{kj} \end{aligned}$$

Since $kj < km = n$, this contradicts the definition of *order* as the lowest n such that $x^n = e$. Therefore, the order of x^k must be exactly m. □

(b) If $x^n = e$, then the order of x divides n.

Proof. Let m be the order of x. By definition of the order of x as the least m such that $x^m = e$, it must be true that $m \leq n$.

Now, let k be the value of n modulo m, so that $n = mj + k$ for some $j \geq 0$, and $0 \leq k < m$. We want to show that $k = 0$. By the fact that $x^n = e$:

$$\begin{aligned} e &= x^n \\ &= x^{mj+k} \\ &= (x^{mj})(x^k) \\ &= (x^m)^j x^k \\ &= e^j x^k \qquad\qquad\qquad\qquad = x^k \end{aligned}$$

So, $x^k = e$. Since $0 \leq k < m$, it must be true that $k = 0$, since otherwise it would contradict the definition of m as the lowest such number. □

(c) If $f : G \to H$ is a homomorphism, then $f(x)$ divides the order of x.

Proof. Let m be the order of x in G. We see that $f(x)^m = f(x^m) = e$. By the previous anser, we see that the order of $f(x)$ must divide m. □

Problem 3. Let H and K be subgroups of G. A *double coset* of (H,K) is a subset HtK, with $t \in G$. Show that the double cosets of (H,K) partition G.

Proof. We show that two double cosets HxK, HyK are either the same, or are disjoint; and also that every element of G belongs to one such double coset, meaning they partition G into a union of disjoint subsets.

First, it is clear that every element $g \in G$ belongs to the double coset HgK, as $g = ege \in HgK$. Now, let $x, y \in G$ be different elements of G such that $HxK \cap HyK \neq \emptyset$. Then there exists some element t such that $t = h_1xk_1 = h_2yk_2$. But then

$$x = h_1^{-1}tk_1^{-1} = h_1^{-1}h_2yk_2k_1^{-1}$$

Therefore, for any $s = h'xk' \in HxK$, the element s is also in HyK:

$$s = h'xk' = (h'h_1^{-1}h_2)y(k_2k_1^{-1}k') \in HyK$$

And symmetrically, every element of HyK is also in HxK, meaning the two sets are equal, and the double cosets partition G. □

If $G = \cup_{i=1}^{n} Ht_iK$, then $|G : K = \sum_i |H : (H \cap t_iKt_i^{-1}|$.

Proof. incomplete □

4 Let a and n be coprime. Show that $a^{\varphi(n)} = 1(\text{mod } n)$. (*Euler*)

Proof. We show that the set P of numbers k, where $1 \leq k \leq n-1$, and $\gcd(n,k) = 1$, is a group under multiplication modulo n. Because $\mathbb{Z}_n$ is a ring, its multiplication operation satisfies associativity and identity already; we only need to see that P is multiplicatively closed, and includes an inverse to every element.

Multiplicative closure: let k, j be two numbers less than n such that $\gcd(j,n) = \gcd(k,n) = 1$. Then $\gcd(kj,n) = 1$ as well, and so the product of k and j, $kj \text{mod} n$, is an element of P.

Let k be some number less than k such that k and n have greatest common divisor 1. It is a theorem of number theory that there must exist integers x, y such that $xk + yn = \gcd(n,k) = 1$. Fix an x, y such that this holds; then $x\text{mod}(n)$ is an inverse to k. Therefore, P is a group. By definition of $\varphi(n)$ as the number of k, where $1 \leq k \leq n-1$ and n and k are coprime, we see that the order of P must be $\varphi(n)$. So, for every natural number $c \in [1, n-1]$ such that a and n are coprime, $b^{\varphi(n)} = 1\text{mod} n$. Because the modular operation commutes with multiplication, and coprime-ness with n is preserved under mod$n$, this extends to every integer a which is coprime with n, proving the theorem. □

In particular, for p prime, $a^{p-1} = 1(\text{mod } p)$. This follows immediately from the fact that, for all $p-1$ integers k such that $1 \leq k < p$, then $\gcd(k,n) = 1$.

Problem 5. If S and T are subsets of a group G, then either $G = ST$ or $|G| \geq |S| + |T|$.

Proof. We want to show that, if $G \neq ST$, then $|G| \geq |S| + |T|$. So, assume that there exists some $g \in G$ such that g cannot be written as st for any $s \in S$, $t \in T$. In particular, $g \neq se$ and $g \neq et$, so it is not an element of G or S. We will use this g to construct a set of at least $|S| + |T|$ elements of G.

Let $U = (gS \cup S) \cup (gT \cup T)$. Since $g \notin S$ and $g \notin T$, the sets gS and S are disjoint, as are the sets gT and T. Therefore the set $(gS \cup S)$ has $2|S|$ elements, and the set $(gT \cup T)$ has $2|T|$. So, the set U has at least $\max(2|S|, 2|T|)$ elements. It is a fact that, for any two nonnegative numbers a, b (finite or infinite), $\max(2a, 2b) \geq a + b$. So, in particular, $|U| \geq |S| + |T|$. Since U is a subset of G, we see that G must have at least $|S| + |T|$ elements. □

Problem 6. (a) If H and K are normal, then $H \cap K$ is normal and $\langle H \cup K \rangle$ is normal.

Proof. We first show that $H \cap K$ is normal. Let $x \in H \cap K$, and let $y \in G$; then $yxy^{-1} \in H$ and $yxy^{-1} \in K$ by normality of H and K; so $yxy^{-1} \in H \cap K$, showing that $H \cap K$ is normal.

Now, we show that $\langle H \cup K \rangle$ is normal. Let $x \in \langle H \cup K \rangle$, and $y \in G$. By definition of $\langle H \cup K \rangle$, there must exist some set of elements $x_1, \ldots, x_n$ such that $x_i \in H \cup K$, and $x = x_1 \cdots x_n$. So we see that, under conjugation, x remains in $\langle H \cup K \rangle$

$$\begin{aligned} yxy^{-1} &= y(x_1 \cdots x_n)y^{-1} \\ &= (yx_1y^{-1}) \cdots (yx_ny^{-1}) \end{aligned}$$

For each x_i, either $x_i \in H$, meaning $yx_iy^{-1} \in H$, or $x_i \in K$, so $yx_i^{-1} \in K$. Either way, $yx_iy^{-1} \in H \cup K$, meaning the product of all yx_iy^{-1} is in $\langle H \cup K \rangle$, and the group is indeed normal in G. □

(b) A subgroup H is normal in G if and only if H is the union of conjugacy classes of G.

Proof. Assume H normal. Then for each $h \in H$, the conjugacy class $C(h) := \{xhx^{-1}; x \in G\} \subset H$, so H is the union of all such $C(h)$. In the opposite direction, if H is the union of conjugacy classes, then every $h \in H$ belongs to one such conjugacy class. Because conjugacy classes are disjoint, this class is unique, and so it must be contained entirely in H - so that $xhx^{-1} \in H$ for all $x \in G$. Since this holds for all $h \in H$, we see that H must be normal. □

Problem 7. Let H be normal in G. if $g \in G$ and $h \in H$, then there exists $k \in H$ such that $gh = kg$ (partial commutativity).

Proof. By normality, we see that $ghg^{-1} = k$ for some $k \in H$. Multiplying both sides on the right by g, we see that $gh = kg$, as was to be shown. □

Problem 8. Let A, B, C be normal subgroups, with $A \subseteq B$.

(a) If $A \cap C = B \cap C$ and $AC = BC$, then $A = B$. (The modular law).

Proof. We show that, for all $b \in B$, then $b \in A$ as well.

Let $b \in B$. Since $b = be \in BC$, then $b \in AC$ as well, meaning there are some $a \in A$ and $c \in C$ such that $b = ac$. Since $a \subseteq B$, we have $c = a^{-1}b \in B$, and so $c \in B \cap C$. By assumption, this shows that $c \in A \cap C$ as well, meaning that $b = ac \in A$. □

(b) $(AC) \cap B = A(C \cap B)$ (Dedekind's law).

Proof. Let $x \in (AC) \cap B$. Then $x = ac$ for some $a \in A$ and $c \in C$, and also $x \in B$. Since $A \subseteq B$, we see that $a \in B$ as well, and so $c = a^{-1}x$ is in B as well as C. Therefore, $c \in C \cap B$, and so $x \in A(C \cap B)$.

Now, assume that $x \in A(C \cap B)$: that $x = a(y)$ for some $y \in (C \cap B)$. Since $y \in C$, $x \in AC$, and since $a \in A \subseteq B$, and $y \in B$, $x \in B$. Therefore, $x \in (AC) \cap B$. So, the two sets are equal. □

Problem 9. If $[G, G] \leq H$. then H is normal in G.

Proof. Let H be a subgroup such that the commutator subgroup of G is contained in H. Let $h \in H$ and $x \in G$; we wish to show that $xhx^{-1} \in H$. But because $xhx^{-1}h^{-1} \in [G, G] \subset H$, we see that $xhx^{-1}h^{-1} \in H$. Since $h \in H$ as well, it follows that $xhx^{-1} = (xhx^{-1}h^{-1})h \in H$. □

Problem 10. If H is normal in G, must G contain a subgroup isomorphic to G/H?

Proof. No, not necessarily. For example, let G be $\mathbb{Z}$ and let H be $2\mathbb{Z}$. then $G/H = \mathbb{Z}/2\mathbb{Z}$. In this case, the group G/H has an element of order 2, while no element of G does, so G cannot contain a subgroup isomorphic to G/H. □

Problem 12. The symmetric group S_n is generated by each of the following:

(a) $(12), (13), \ldots, (1n)$

Proof. We want to show that any permutation can be generated by the transpositions $(12), (13), \ldots, (1n)$. Since any permutation is the product of cycles, it suffices to show that every cycle can be generated by these transpositions. We will proceed by induction on the length of the cycle.

First, let $x = (a, b)$ be a cycle of length 2. We see that $(a, b) = (1, a)(1, b)(1, a)$, as this takes

$$\begin{gathered} 1 \to a \to 1 \\ a \to 1 \to b \\ b \to 1 \to a \end{gathered}$$

Therefore, every cycle of length 2 can be generated by these transpositions. Now, assume that every cycle of length $k - 1$ can be generated by transpositions, and let $x = (a_1, a_2, \ldots, a_k)$ be a cycle of length k. We can decompose x as

$$(a_1, a_2, \ldots, a_k) = (1, a_1)(1, a_{k-1})(1, a_k)(1, a_1)(a_1, a_2, \ldots, a_{k-1})$$

This decomposition works correctly on each element:

$$\begin{aligned} 1 &\to a_1 \to 1 \\ a_1 &\to a_2 \\ &\vdots \\ a_{k-2} &\to a_{k-1} \\ a_{k-1} &\to a_1 \to 1 \to a_k \\ a_k &\to 1 \to a_1 \end{aligned}$$

By the inductive hypothesis, the cycle $(a_1, \ldots, a_{k-1})$ can also be decomposed as a product of transpositions $(1k)$. Induction shows that every cycle in S_n can be generated by these transpositions, and so every generic element of S_n can be generated by them. □

(b) $(12), (23), \ldots, (i, i+1), \ldots, (n-1, n)$

Proof. By the preceding proof, it suffices to show that any transposition $(1k)$ can be decomposed into transpositions $(i, i+1)$. Let $x = (1k)$, where $k \neq 1$: we can decompose x as

$$(1k) = (12)(23) \cdots (k-2, k-1)(k-1, k)(k-2, k-1) \cdots (23)(12)$$

This works correctly on every element from 1 to k:

$$\begin{aligned} 1 &\to 2 \to \cdots \to k \\ 2 &\to 1 \to 2 \\ 3 &\to 2 \to 3 \\ &\vdots \\ (k-1) &\to (k-2) \to (k-1) \\ k &\to (k-1) \to \cdots \to 1 \end{aligned}$$

So it fixes every element of $1, \ldots, n$ except for 1 and k, which it switches. Since the transpositions $(1k)$ generate S_n, so do the transpositions $(i-1, i)$. □

(c) (12) and $(12 \cdots n)$.

Proof. By the previous proof, it suffices to show that any $(i, i+1)$ can be written as a product of the transposition (12) and the n-cycle $(12 \ldots n)$. Let $i \geq 3$; we want to decompose $(i, i+1)$. We see that $(12\dots n)^i(12)(12\dots n)^{-i}$ works, as it takes

$$\begin{aligned}
1 &\to n \to (n-1) \to \cdots \to (n-i) \to (n-i+1) \to \cdots n \to 1\\
2 &\to 1 \to \cdots \to (n-i+1) \to (n-1+2) \to \cdots 1 \to 2\\
&\vdots\\
i &\to (i-1) \to \cdots \to \mathbf{1} \to \mathbf{2} \to 3 \to \cdots \to i \to (i+1)\\
(i+1) &\to i \to \cdots \to \mathbf{2} \to \mathbf{1} \to 2 \to \cdots \to (i-1) \to i\\
&\vdots\\
n &\to (n-1) \to \cdots \to (n-i-1) \to (n-i) \to \cdots \to (n-1) \to n
\end{aligned}$$

Where the boldfaced numbers indicate the only time the transposition (12) acts on an element. Since this acts correctly on every number from 1 to n, it is equal to the transposition $(i, i+1)$; and, since these transpositions generate S_n, so do the two cycles (12) and $(12\cdots n)$. □

Problem 13. The alternating group A_n is generated by the 3-cycles; $n \geq 3$.

Proof. Every 3-cycle is a member of the alternating group, since it can be decomposed as a pair of transpositions:

$$(abc) = (ac)(ab)$$

Since the alternating group is generated by pairs of transpositions, it suffices to show that every pair of transpositions can be written as the product of 3-cycles. Let $x = (ab)(cd)$ be an arbitrary pair of transpositions; then x can be decomposed as

$$(ab)(cd) = (cad)(abc)$$

This is the correct decomposition, as it acts correctly on all four elements:

$$\begin{aligned}
&a \to b\\
&b \to c \to a\\
&c \to a \to d\\
&d \to c
\end{aligned}$$

So, every pair of transpositions can be written as the product of 3-cycles, and so the whole alternating group is generated by the 3-cycles. □

Problem 14. If $G \leq S_n$ and G contains an odd permutation, then exactly half of the elements of G are odd permutations.

Proof. Let $G \leq S_n$ be a group containing an odd permutation s. Let the set of odd permutations in G be $G_{odd} = \{s, s_1, \dots, s_k\}$, a set with $k+1$ elements. We see that the set $H = \{s^2, ss_1, \dots, ss_k\}$, consisting of the product of s with every odd permutation, consists only of even permutations, as the product of two odd permutations is an even permutation. Each permutation in it must be unique, because if $ss_i = ss_j$, then $s^{-1}ss_i = s^{-1}ss_j$ implies that $s_i = s_j$. Finally, we see that every even permutation in G must be in this set, because if $t \in G$ is even, then $t = s(s^{-1}t)$, where $s^{-1}t$ is an odd permutation. Therefore, the two sets G_{odd} and H partition G into two subsets of equal size: exactly half of the elements of G are odd permutations. □

Problem 15. If G is a group of order $2n$, with n odd, then G has a subgroup of order n.

Proof. (Skeleton of proof found on math.stackexchange.com) Since the prime 2 divides the order of G, there must be a subgroup H of G of order 2. Let $N_G(H)$ be the normalizer of H, and $C_G(H)$ its centralizer. We know that $C_G(H)$ is a normal subgroup of $N_G(H)$, and that $N_G(H)/C_G(H)$ is a subgroup of Aut(H). But, since H is of order 2, it is isomorphic to $\mathbb{Z}_2$, which has trivial automorphism group; and so $N_G(H)/C_G(H)$ must be trivial as well. This implies that $C_G(H) = N_G(H)$, meaning that H is in the center of G.

We want to use this to find a subgroup of G that is a normal complement to H: a subgroup K such that $H \cap K = \{e\}$, that $HK = G$, and that K is itself normal. Such a group exists, but I am at a loss as to how to prove it does. *incomplete* □

Problem 16. If G is a group that contains a subgroup of index p, where p is the smallest prime that divides the order of G, then this subgroup is normal in G.

Proof. (From math.stackexchange.com) Let H be a subgroup of index p in G, where p is the smallest prime dividing the order of G. The set of cosets of H has size p, and G acts on them by left multiplication: $x \cdot gH = (xg)H$. Thus each element permutes the cosets of H, giving a nontrivial map from G to the symmetric group S_p, whose kernel is contained in H (since H acts trivially on its own cosets).

Let K be the kernel of this map. Since $|G/K| \leq S_p$, it must have order dividing $|S_p| = p!$. But it must also have order dividing $|G|$. Since p is the smallest prime dividing $|G|$, it is the only nontrivial factor of both $p!$ and $|G|$; therefore, G/K must have order p.

We see that $|G/K| = [G : K] = [G : H][H : K] = p[H : K]$, from which follows $[H : K] = 1$; i.e. that $H = K$. Since K is normal, we have proved the theorem. □

Problem 17. A nonidentity normal subgroup of a p-group intersects the center of the p-group in more than one element.

Proof. (From math.stackexchange.com) First, we first see that any conjugacy class of a p-group must have order p^k for some k: this is because $|\mathrm{Cl}(g)| = |G| \,/\, |C_G(g)|$, where $\mathrm{Cl}(g)$ is the conjugacy class of G and $C_G(g)$ is its centralizer (this is proved in Dummit & Foote). Since $|G| = p^n$ for some n, and $|C_G(g)| = p^m$ for some $m \leq n$, it follows that $|\mathrm{Cl}(g)| = p^{n-m}$.

Now, let H be a nonidentity normal subgroup of G, and let $Z(G)$ be the center of G. Since H is not the identity, it has order p^l for some $l \geq 1$, and it contains the trivial conjugacy class $\{e\}$ of order 1, it must contain at least $p - 1$ other conjugacy classes of order 1, and any element with a conjugacy class of order 1 is an element of the center of G. Thus there are at least p elements of $Z(G)$ contained in H. □

Problem 18. Every proper subgroup of order p^k of a p-group can be imbedded in a subgroup of order p^{k+1}. Conclude that the maximal subgroups in a p-group are all of index p.

Proof. incomplete. □

Problem 19. For each prime that divides $|G|$ select a Sylow p-subgroup of G. Show that these Sylow p-subgroups generate G.

Proof. First, we see that if H is a Sylow p_1-subgroup, and K is a Sylow p_2-subgroup, $p_1 \neq p_2$, then $H \cap K$ must be trivial; for $|H \cap K|$ divides both $|H| = p_i^n$ and $|K| = p_2^m$, which are coprime. So, by the fact that $\langle H \cup K \rangle \subset HK$, and the earlier theorem that $|HK|\,|H \cap K| = |H|\,|K|$, we see that $|\langle H \cup K \rangle| = p_1^n p_2^m$.

Generalizing, if two subgroups have coprime order, then the order of the group generated by their union has order equal to the product of the two groups' orders. So, if $H_1, H_2, \ldots, H_j$ are the Sylow p-subgroups of G chosen in the hypothesis, the order of $\langle H_1 \cup H_2 \cup \cdots \cup H_j \rangle$ is equal to the product of their orders. And, because $|H_i| = p_i^m$, where p_i^m is the highest power of p_i dividing $|G|$, we see by examining the prime factors of $|G|$ that the order of G and the order of $\langle H_1 \cup H_2 \cup \cdots \cup H_j \rangle$ must be equal, and so the Sylow subgroups do indeed generate G. □

Problem 20. Any subgroup that contains the normalizer of a Sylow p-subgroup is self-normalizing; that is, its normalizer is equal to itself.

Proof. incomplete □