MATH1530, HOMEWORK 6

Section 3.2

4. Show that if $|G| = pq$ for some primes p and q then either G is abelian or $Z(G) = 1$.

Last week, we have seen that if $G/Z(G)$ is cyclic, then G is abelian. From Lagrange's theorem, $|Z(G)|$ is either 1, p, q, or pq. Assume it is not equal to 1. Then $G/Z(G)$ is either $pq/p = q$, $pq/q = p$, or $pq/pq = 1$. In any case, this group is cyclic, and therefore G is abelian.

7. Let $H \leq G$ and define a relation $\sim$ on G by $a \sim b$ if and only if $b^{-1}a \in H$. Prove that $\sim$is an equivalence relation and describe the equivalence class of each $a \in G$.

(i) Reflexive: $a \sim a$ because $a^{-1}a = 1 \in H$
(ii) Symmetric: $a \sim b$ implies $b^{-1}a \in H$, which means $(b^{-1}a)^{-1} = a^{-1}b \in H$, showing $b \sim a$
(iii) Transitive: $a \sim b$ and $b \sim c$ implies $b^{-1}a, c^{-1}b \in H$, and by multiplying we get $c^{-1}a \in H$.

We claim that for any $a \in G$, the equivalence class of a is precisely $aH = \{ah : h \in H\}$. For a moment assume $a \sim b$, or $b^{-1}a \in H$. It means $b^{-1}a = h$ for some $h \in H$. Again, it is equivalent to $b = ah^{-1} \in aH$. On the other hand if $c \in aH$ it means $c = ah'$ for some $h' \in H$. Then $a^{-1}c \in H$, showing $a \sim c$.

Proposition 4 says that the set of left cosets of N in G form a partition of G. This is clear now, since any equivalence relation form a partition of the set where each equivalence class is a left coset of some element. Furthermore, $uN = vN$ implies u and v are in the same equivalence class, or $u^{-1}v \in N$. Hence this is also obvious.

8. Prove that if H and K are finite subgroups of G whose orders are relatively prime then $H \cap K = 1$.

The intersection $H \cap K$ is a subgroup, as we have seen before. Then from Lagrange's theorem, $|H \cap K|$ should divide $|H|$ and $|K|$. But since $|H|$ and $|K|$ are relatively prime, $|H \cap K| = 1$ or $H \cap K = \{1\}$.

12. Let $H \leq G$. Prove that the map $x \mapsto x^{-1}$ sends each left coset of H in G onto a right coset of H and gives a bijection between the set of left cosets and the set of right cosets of H in G.

Let aH be a left coset, and we consider the image of this set under the map $x \mapsto x^{-1}$. Any element in aH is of the form ah, and it is mapped to $(ah)^{-1} = h^{-1}a^{-1}$. Therefore, the image of aH is contained in the right coset Ha^{-1}. On the other hand, if we have $y \in Ha^{-1}$ then $y = h'a^{-1}$ for some $h' \in H$ and since $y^{-1} \mapsto y$ and $y^{-1} = ah'^{-1}$, $ah'^{-1} \mapsto y$, showing that this map establishes a bijection between aH and Ha^{-1}.

That is, this map defines a correspondence on the set of left cosets to the set of right cosets by $aH \mapsto Ha^{-1}$. Assume aH and bH has the same image, which means $Ha^{-1} = Hb^{-1}$, or $a^{-1}b \in H$. Then $aH = bH$, showing that this correspondence is injective. On the other hand, given any right coset Hg, $g^{-1}H \mapsto Hg$, showing this correspondence is surjective.

18. Let G be a finite group, let H be a subgroup of G and let $N \trianglelefteq G$. Prove that if $|H|$ and $|G : N|$ are relatively prime then $H \leq N$.

Since G is finite, consider the unique prime decomposition of $|G|$, $|G| = p_1^{a_1}p_2^{a_2}...p_n^{a_n}$ where p_i are distinct primes and $1 \leq a_i$ for all $1 \leq i \leq n$. By re-indexing the primes if necessary, we can assume $|H| = p_1^{b_1}p_2^{b_2}...p_k^{b_k}$, where we can guarantee that $k \leq n$ and $1 \leq b_i \leq a_i$ for all $i \leq k$. Since $|G : N| = \frac{|G|}{|N|}$, and this is relatively prime with $|H|$, so it is forced that $|N|$ divides $p_1^{a_1}p_2^{a_2}...p_k^{a_k}$. Otherwise, some powers of p_j for $j \leq k$ will remain on $|G|/|N|$ and therefore p_j will divide the greatest common divisor of $|H|$ and $|G|/|N|$, which is a contradiction.

Next, we observe that since N is a normal subgroup, NH is also a subgroup of G and hence $|NH|$ should divide $|G|$. But we claim that $|NH|$ divides $|N|$, which is striking. If we look at primes $p_1, ..., p_k$, $|NH|$ cannot contain more than a_i powers of p_i for $i \leq k$ simply because $|NH|$ should be divisible by $|G|$ and $|G|$ only has a_i powers of p_i. However, $|N|$ contains exactly a_i powers of p_i. Now we look at primes $p_{k+1}, ..., p_n$. From the formula

$$|NH| = \frac{|N| \cdot |H|}{|N \cap H|},$$

we notice that $|NH|$ never contains more powers of p_j $(k+1 \leq j)$ than $|N|$ does, since $|H|$ does not contain powers of p_j $(k+1 \leq j)$ at all. That is, $|NH|$ divides $|N|$. But it is obvious that N is a subgroup of NH, so $|NH| = |N|$, and from above formula,

$$1 = \frac{|H|}{|N \cap H|}$$

showing that $|N \cap H| = |H|$, or $N \cap H = H$, or $H \subseteq N$, or $H \leq N$. We are done.

19. Prove that if N is a normal subgroup of the finite group G and $(|N|, |G : N|) = 1$ then N is the unique subgroup of G of order $|N|$.

Let H be a subgroup of G of order $|H| = |N|$. Then $(|H|, |G : N|) = 1$ and from above exercise, $H \leq N$, but cardinality condition forces $H = N$.

22. Use Lagrange's theorem in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ to prove Euler's Theorem: $a^{\phi(n)} \equiv 1 \bmod n$ for every integer a relatively prime to n, where ϕ denotes Euler's ϕ-function.

For any element $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$, we consider the subgroup generated by $\bar{a}$, say A. Then $|A|$ divides the order of $(\mathbb{Z}/n\mathbb{Z})^\times = \phi(n)$. But $\bar{a}^{|A|} = 1$ as A is the cyclic group generated by $\bar{a}$. Then for a stronger reason, $\bar{a}^{\phi(n)} = 1$, or $a^{\phi(n)} \equiv 1 \bmod n$.

Section 3.3

3. Prove that if H is a normal subgroup of G of prime index p then for all $K \leq G$ either
(i) $K \leq H$ or
(ii) $G = HK$ and $|K : K \cap H| = p$.

It is enough to assume that given a subgroup K of G, (i) is false and then show (ii) is true.

So we are assuming $K \not\leq H$. Now HK is a subgroup since H is normal and we have obvious inclusions $H \leq HK \leq G$. In particular, from Lagrange's theorem, $|G|/|H|$ should be divisible by $|G|/|HK|$. But since $|G|/|H| = p$, $|G|/|HK|$ is 1 or p but if this is 1 then $G = HK$ and otherwise $HK = H$, a contradiction to $K \not\leq H$. That is, $G = HK$. Then

$$|G| = \frac{|K| \cdot |H|}{|K \cap H|}$$

or equivalently

$$p = \frac{|G|}{|H|} = \frac{|K|}{|K \cap H|}$$

so we are done.

4. Let C be a normal subgroup of the group A and let D be a normal subgroup of the group B. Prove that $(C \times D) \trianglelefteq (A \times B)$ and $(A \times B)/(C \times D) \cong (A/C) \times (B/D)$.

(1) $(C \times D) \trianglelefteq (A \times B)$

By definition, we need to show that for any $g \in A \times B$ and $x \in C \times D$, $gxg^{-1} \in C \times D$. Any such g is of the form (a, b) where $a \in A$ and $b \in B$. Likewise, $x = (c, d)$ for some $c \in C$ and $d \in D$. We have $g^{-1} = (a^{-1}, b^{-1})$ by definition of a product group, and then we compute

$$gxg^{-1} = (a, b)(c, d)(a^{-1}, b^{-1}) = (aca^{-1}, bdb^{-1})$$

but since C is normal in A, $aca^{-1} \in C$ and likewise $bdb^{-1} \in D$. That is, $(aca^{-1}, bdb^{-1}) \in C \times D$.

(2) $(A \times B)/(C \times D) \cong (A/C) \times (B/D)$

There is essentially only one thing we can do to prove a statement like this. We build a surjective homomorphism $\phi : A \times B \to (A/C) \times (B/D)$ and show that its kernel is precisely $C \times D$.

And this homomorphism will be simply a product of projections: $\phi(a, b) := (aC, bD)$. We need to show this is a homomorphism: $\phi(a, b)\phi(a', b') = (aC, bD) \cdot (a'C, b'D) = (aa'C, bb'D) = \phi(aa', bb') = \phi\{(a, b) \cdot (a', b')\}$. This is surjective, because by definition any element of $(A/C) \times (B/D)$ has the form (aC, bD) for some $a \in A$ and $b \in B$. Then we ask what the kernel is. $(a, b) \in \ker \phi$ if and only if $aC = C$ and $bD = D$ as (C, D) is the identity element of $(A/C) \times (B/D)$. But $aC = C$ is equivalent to $a \in C$ and likewise, we have $b \in D$. That is, (a, b) is in kernel if and only if $a \in C$ and $b \in D$, or $(a, b) \in C \times D$. Hence we are done.

6. Let $M =< v, u >$ be the modular group of order 16 described in Exercise 14 of section 2.5. Prove that $< v^4 >$ is normal in M and use the Lattice Isomorphism Theorem to draw the lattice of subgroups of $M/ < v^4 >$. Which group of order 8 has the same lattice as this quotient? Use generators and relations for $M/ < v^4 >$ to decide the isomorphism type of this group.

(1) $< v^4 >$ is normal.

Any element of M is uniquely represented by $u^i v^j$ where $i \in \{0, 1\}$ and $j \in \{0, 1, ..., 7\}$. Therefore, $gv^4g^{-1} = u^i v^j v^4 v^{-j} u^{-i} = u^i v^4 u^{-i}$ and if i were 0 we are done and otherwise $uv^4u = uv^3uv^5 = uv^2uv^{10} = uvuv^{15} = u^2v^{20} = v^4$. Hence this subgroup is normal.

Next, compare this diagram with the lattice of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$:

If you stare at these two diagrams long enough, you will be convinced that they are isomorphic, with $\bar{u} = (1, 0)$ and $\bar{v} = (0, 1)$.

7. Let M and N be normal subgroups of G such that $G = MN$. Prove that

$$G/(M \cap N) \cong (G/M) \times (G/N).$$

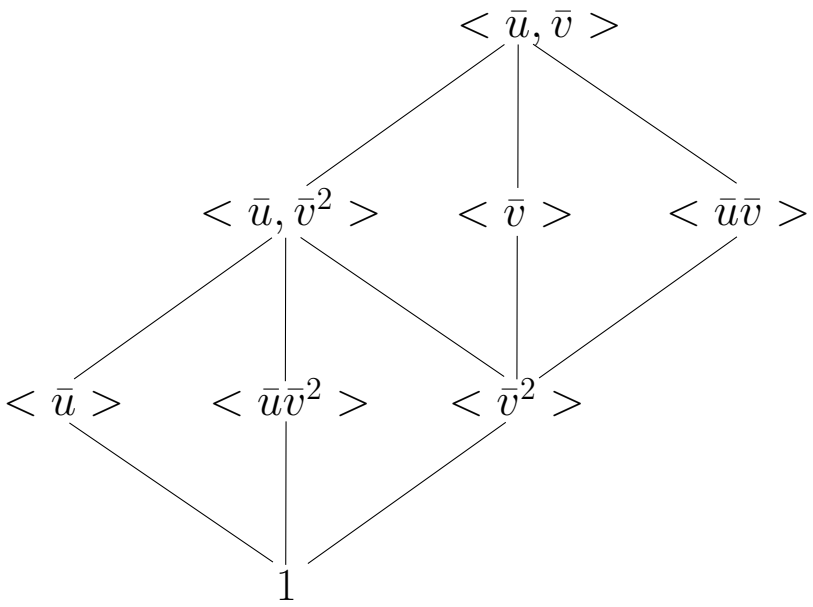

FIGURE 0.1

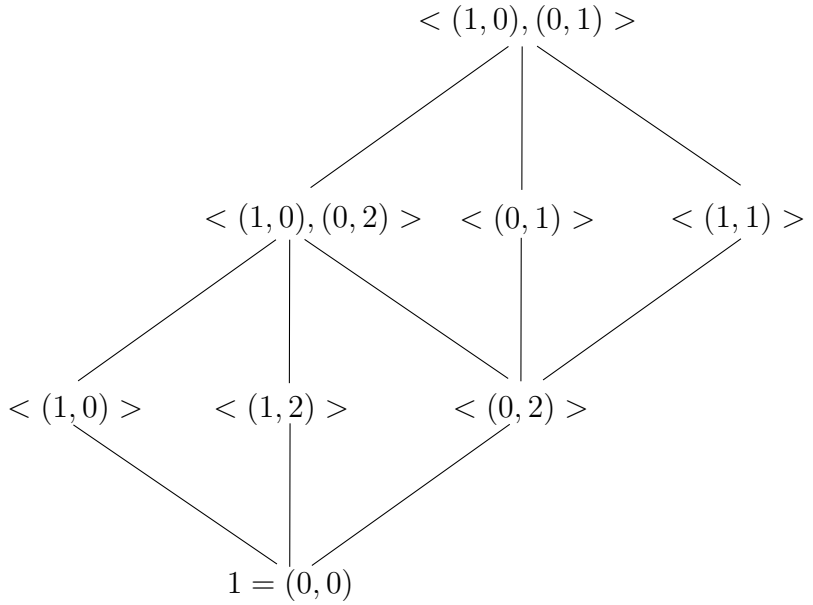

FIGURE 0.2

We define $\phi : G \mapsto (G/M) \times (G/N)$ by $\phi(g) = (gM, gN)$ (this is the only option we have). Then this is a homomorphism, and g is in the kernel if and only if $g \in M$ and $g \in N$, or $g \in M \cap N$. Finally we want to show it is surjective. Any elment in the range is of the form (gM, hN) for some $g, h \in G$. We want to find $x \in G$ such that $xM = gM$ and $xN = hN$. But any $g \in G$ is a product $g = mn$ where $m \in M$ and $n \in N$. Clearly, $gM = mnM = nM$ because $mn \cdot n^{-1} = m \in M$ and they define the same coset. Likewise, if we have the product $h = m'n'$ then $hN = m'n'N = m'N$. If we put $x = nm' \in G$ then $xM = nm'M = nM = gM$ and $xN = nm'N = m'N = hN$, so ϕ is surjective.