(*January 14, 2009*)

[02.1] Let G, H be finite groups with relatively prime orders. Show that any group homomorphism $f : G \to H$ is necessarily trivial (that is, sends every element of G to the identity in H.)

The isomorphism theorem implies that

$$|G| = |\ker f| \cdot |f(G)|$$

In particular, $|f(G)|$ divides $|G|$. Since $f(G)$ is a subgroup of H, its order must also divide $|H|$. These two orders are relatively prime, so $|f(G)| = 1$.

[02.2] Let m and n be integers. Give a formula for an isomorphism of abelian groups

$$\frac{\mathbb{Z}}{m} \oplus \frac{\mathbb{Z}}{n} \to \frac{\mathbb{Z}}{\gcd(m,n)} \oplus \frac{\mathbb{Z}}{\mathrm{lcm}(m,n)}$$

Let r, s be integers such that $rm + sn = \gcd(m,n)$. Let $m' = m/\gcd(m,n)$ and $n' = n/\gcd(m,n)$. Then $rm' + sn' = 1$. We claim that

$$f(a + m\mathbb{Z}, b + n\mathbb{Z}) = ((a-b) + \gcd(m,n)\mathbb{Z},\ (b \cdot rm' + a \cdot sn') + \mathrm{lcm}(m,n)\mathbb{Z})$$

is such an isomorphism. To see that it is well-defined, observe that

$$(a + m\mathbb{Z}) - (b + n\mathbb{Z}) = (a-b) + \gcd(m,n)\mathbb{Z}$$

since

$$m\mathbb{Z} + n\mathbb{Z} = \gcd(m,n)\mathbb{Z}$$

which itself follows from the facts that

$$\gcd(m,n) = rm + sn \in m\mathbb{Z} + n\mathbb{Z}$$

and (by definition) $m\mathbb{Z} \subset \gcd(m,n)\mathbb{Z}$ and $n\mathbb{Z} \subset \gcd(m,n)\mathbb{Z}$. And, similarly

$$sn' \cdot m\mathbb{Z} + rm' \cdot n\mathbb{Z} = \mathrm{lcm}(m,n)\mathbb{Z}$$

so the second component of the map is also well-defined.

Now since these things are finite, it suffices to show that the kernel is trivial. That is, suppose $b = a + k\gcd(m,n)$ for some integer k, and consider

$$b \cdot rm' + a \cdot sn'$$

The latter is

$$(a + k\gcd(m,n))rm' + a \cdot sn' = a \cdot rm' + a \cdot sn' = a \bmod m$$

since $\gcd(m,n)m' = m$ and $rm' + sn' = 1$. Symmetrically, it is $b \bmod n$. Thus, if it is $0 \bmod \mathrm{lcm}(m,n)$, $a = 0 \bmod m$ and $b = 0 \bmod n$. This proves that the kernel is trivial, so the map is injective, and, because of finiteness, surjective as well.

[0.0.1] **Remark:** I leave you the fun of guessing where the $a - b$ expression (above) comes from.

[02.3] Show that every group of order $5 \cdot 13$ is cyclic.

Invoke the Sylow theorem: the number of 5-Sylow subgroups is 1 mod 5 and also divides the order $5 \cdot 13$, so must be 1 (since 13 is not 1 mod 5). Thus, the 5-Sylow subgroup is normal. Similarly, even more easily, the 13-Sylow subgroup is normal. The intersection of the two is trivial, by Lagrange. Thus, we have two normal subgroups with trivial intersection and the product of whose orders is the order of the whole group, and conclude that the whole group is isomorphic to the (direct) product of the two, namely $\mathbb{Z}/5 \oplus \mathbb{Z}/13$. Further, this is isomorphic to $\mathbb{Z}/65$.

[02.4] Show that every group of order $5 \cdot 7^2$ is abelian.

From the classification of groups of prime-squared order, we know that there are only two (isomorphism classes of) groups of order 7^2, $\mathbb{Z}/49$ and $\mathbb{Z}/7 \oplus \mathbb{Z}/7$. From the Sylow theorem, since the number of 7-Sylow subgroups is 1 mod 7 and also divides the group order, the 7-Sylow subgroup is normal. For the same reason the 5-Sylow subgroup is normal. The intersection of the two is trivial (Lagrange). Thus, again, we have two normal subgroups with trivial intersection the product of whose orders is the group order, so the group is the direct product. Since the factor groups are abelian, so is the whole.

[02.5] Exhibit a non-abelian group of order $3 \cdot 7$.

We can construct this as a semi-direct product, since there exists a non-trivial homomorphism of $\mathbb{Z}/3$ to $\mathrm{Aut}(\mathbb{Z}/7)$, since the latter automorphism group is isomorphic to $(\mathbb{Z}/7)^\times$, of order 6. Note that we are assured of the *existence* of a subgroup of order 3 of the latter, whether or not we demonstrate an explicit element.

[02.6] Exhibit a non-abelian group of order $5 \cdot 19^2$.

We can construct this as a semi-direct product, since there exists a non-trivial homomorphism of $\mathbb{Z}/5$ to $\mathrm{Aut}(\mathbb{Z}/19 \oplus \mathbb{Z}/19)$, since the latter automorphism group has order $(19^2 - 1)(19^2 - 19)$, which is divisible by 5. Note that we are assured of the *existence* of a subgroup of order 5 of the latter, whether or not we demonstrate an explicit element.

[02.7] Show that every group of order $3 \cdot 5 \cdot 17$ is cyclic.

Again, the usual divisibility trick from the Sylow theorem proves that the 17-group is normal. Further, since neither 3 nor 5 divides $17 - 1 = |\mathrm{Aut}(\mathbb{Z}/17)|$, the 17-group is *central.* But, since $3 \cdot 17 = 1 \bmod 5$, and $5 \cdot 17 = 1 \bmod 3$, we cannot immediately reach the same sort of conclusion about the 3-group and 5-group. But if *both* the 3-group and 5-group were *not* normal, then we'd have at least

$$1 + (17-1) + (5-1) \cdot 3 \cdot 17 + (3-1) \cdot 5 \cdot 17 = 391 > 3 \cdot 5 \cdot 17 = 255$$

elements in the group. So at least one of the two is normal. If the 5-group is normal, then the 3-group acts trivially on it by automorphisms, since 3 does not divide $5 - 1 = |\mathrm{Aut}(\mathbb{Z}/5)|$. Then we'd have a *central* subgroup of order $5 \cdot 17$ group, and the whole group is abelian, so is cyclic by the type of arguments given earlier. Or, if the 3-group is normal, then for the same reason it is is central, so we have a central (cyclic) group of order $3 \cdot 17$, and again the whole group is cyclic.

[02.8] Do there exist 4 primes p, q, r, s such that every group of order $pqrs$ is necessarily abelian?

We want to arrange that all of the p, q, r, s Sylow subgroups P, Q, R, S are normal. Then, because the primes are distinct, still

$$P \cap Q = \{e\}$$

$$P \cdot Q \cap R = \{e\}$$

$$P \cdot Q \cdot R \cap S = \{e\}$$

(and all other combinations) so these subgroups commute with each other. And then, as usual, the whole group is the direct product of these Sylow subgroups.

One way to arrange that all the Sylow subgroups are normal is that, mod p, none of q, r, s, qr, qs, rs, qrs is 1, and symmetrically for the other primes. Further, with none of q, r, s dividing $p - 1$ the p-group is *central.* For example, after some trial and error, plausible $p < q < r < s$ has $p = 17$. Take $q, r, s \bmod 11 = 2, 3, 5$

respectively. Take $q = 13$, so $p = -2 \bmod 13$, and require $r, s = 2, 5 \bmod q$. Then $r = 3 \bmod 11$ and $r = 2 \bmod 13$ is $80 \bmod 143$, and 223 is the first prime in this class. With $s = 5 \bmod 223$, none of the 7 quantities is $1 \bmod r$.. Then $s = 5 \bmod 11 \cdot 13 \cdot 223$ and the first prime of this form is

$$s = 5 + 6 \cdot 11 \cdot 13 \cdot 223 = 191339$$

By this point, we know that the p, q, and r-sylow groups are central, so the whole thing is cyclic.