Assignment 3, Math 4GR3
Due Mar. 14, uploaded to Avenue

1. Let's finish the analysis of a group of order 12 started in class. Recall that we argued that if G has order 12 then it must have either a 2-Sylow normal subgroup N of size 4 or a 3-Sylow normal subgroup of size 3. Let H be a 3-Sylow (respectively 2-Sylow) subgroup in these two cases and note that $G = NH$. In both cases, H will act on N by conjugation so there is a homomorphism $\varphi\colon H \to Aut(N)$. In class we also said that if this homomorphism was trivial i.e. was identically equal to the identity element then $G \cong N \times H$ and so we would be looking at one of two possible abelian examples: $C_2 \times C_2 \times C_3$ and $C_4 \times C_3$. We concentrate then on the cases where φ is not trivial.

    (a) Case 1: In this case, let's suppose that H is of size 3 and N is normal of size 4. So $H \cong C_3$ and N is isomorphic to C_4 or $C_2 \times C_2$. Show that the automorphism group of C_4 is isomorphic to C_2 and conclude there is no non-trivial homomorphism from H to $Aut(N)$ in this case. Now we consider the automorphism group of $C_2 \times C_2$. Conclude that it is non-abelian of size 6 and hence is S_3. Describe a non-trivial homomorphism from C_3 to S_3 and argue, up to isomorphism, there is only one such. Use this information to write down a group of order 12.

    (b) Case 2: In this case, suppose that H has size 4 and N is normal of size 3. So H is isomorphic to $C_2 \times C_2$ or C_4 and $Aut(N)$ is isomorphic to C_2. In each of these cases, convince yourself that up to isomorphism there is only one non-trivial homomorphism from H to $Aut(N)$ and write down the two non-abelian groups of order 12 that arise.

    Solution I'll repeat things said above so that you will have everything in one place:

    (a) Suppose that G is a group with 12 elements. There is a 2-Sylow subgroup of size 4 and a 3-Sylow subgroup of size 3. We showed in class using the third Sylow theorem that either the 3-Sylow subgroup is normal or there are exactly 4 3-Sylow subgroups. In the latter case, the 2-Sylow subgroup is normal. From this we conclude that there are Sylow subgroups A and B such that $G =$

AB and A is a normal subgroup. It follows that G is a semi-direct product of A with B. It is possible that B is also normal which we will consider as part of the cases below.

(b) Case 1: Assume that A is a 3-Sylow subgroup. Then the automorphism group of A is isomorphic to C_2 (the automorphisms are the identity map and the map that sends x to $-x$). B has size 4 and so is abelian i.e. B is isomorphic to $C_2 \times C_2$ or C_4. In order to determine what possible semi-direct products we get in this situation then, we need to determine what possible homomorphisms φ we could have from B to $Aut(A)$ so, up to isomorphism, from $C_2 \times C_2$ or C_4 to C_2. The first possibility is that φ is trivial i.e. always gives us the identity map. In this case then G is just $A \times B$ and so is abelian. In this way, up to isomorphism, we get $C_3 \times C_2 \times C_2$ or $C_3 \times C_4$.

(c) Still in case 1: Now suppose that we are considering B to be $C_2 \times C_2$. If φ is not trivial then it is onto in this case and has a kernel of size 2. Up to isomorphism, we can assume that φ is the projection onto the first coordinate. So $G \cong C_3 \rtimes_\varphi (C_2 \times C_2)$ which one can see is $S_3 \times C_2$. We don't need this last statement (although it is true) since the critical thing is that G is non-abelian and G/A is isomorphic to $C_2 \times C_2$.

(d) If B is isomorphic to C_4 then there is, up to isomorphism, only one non-trivial homomorphism from C_4 to C_2 and so with this choice of φ we obtain $G \cong C_3 \rtimes_\varphi C_4$. This is non-abelian and G/A is isomorphic to C_4.

(e) Case 2: The 2-Sylow subgroup is normal. This would mean that A is isomorphic to $C_2 \times C_2$ or C_4 and B is isomorphic to C_3. Again, what matters are homomorphisms φ from B to $Aut(A)$. If φ is trivial then as above, the product is actually direct and G is abelian. We have characterized all the abelian cases up to isomorphism so let's assume that φ is non-trivial. If we consider the case where A is C_4 then $Aut(C_4)$ is C_2. There is no non-trivial homomorphism from C_3 to C_2 (elements of order 3 would have to go to elements of order 3) and so this case does not occur.

(f) The remaining case is when A is $C_2 \times C_2$ and B is C_3. The automorphism group of $C_2 \times C_2$ is S_3. The sophisticated way to see this is that this is a vector space of dimension 2 over the field with 2 elements. The automorphisms then are just 2 x 2 matrices with non-zero determinant. Less theoretically, any two non-zero elements of $C_2 \times C_2$ act as generators of this group. If e_1 and e_2 are the two standard generators then there are 3 choices where an automorphism could send e_1 and then 2 places it could send e_2. This means that the automorphism group has size 6 and easily it is not abelian so it is S_3. Now up to isomorphism, there is only one non-trivial map from C_3 to S_3 (it sends a generator of C_3 to a 3-cycle in S_3. If we call this map φ then $G \cong A \rtimes_\varphi B$ and its isomorphism type is determined by the fact that A is isomorphic to $C_2 \times C_2$ and G is non-abelian.

2. Show that H_8 is not a semi-direct product. H_8 is the quaterion group and contains 8 elements: $\{\pm 1, \pm i, \pm j, \pm k\}$ and satisfies the following rules

   $(-1)^2 = 1, i^2 = j^2 = k^2 = -1, ij = k = -ji, jk = i = -kj$ and $ki = j = -ik$.

   Hint: If $H_8 \cong N \rtimes A$ then there is a normal subgroup of H_8, let's also call it N; how big is it? Show that if N were of size 2 then H_8 would be abelian (which it is not). Then argue that it can't be of size 4 by looking at elements of order 2.

   Solution As the hint says, how big is N? If N has size 2 then $N \cong C_2$ and $Aut(N)$ is the trivial group. This would mean that the semi-direct product would be direct and H_8 would be abelian (which it is not). So this leaves the possibility that N has size 4 and H has size 2. But then N would contain an element of order 2 (N would be either isomorphic to C_4 or $C_2 \times C_2$). But among the 8 elements of H_8, only -1 has order 2 so this element must be in N. But H also contains an element of order 2 so H is contained in N which it can't be if we have a semi-direct product. So H_8 cannot be represented as a semi-direct product.

3. Judson, chapter 17, # 18: Let $p(x) = a_n x^n + \ldots + a_1 x + a_0$ be an integer polynomial and suppose that $p(r/s) = 0$ for integers r and s with gcd 1. Show that r divides a_0 and s divides a_n.

   Solution: We are given

$$a_n(\frac{r^n}{s^n}) + \ldots + a_1 \frac{r}{s} + a_0 = 0.$$

Multiply through by s^n to get

$$a_n r^n + \ldots + r s^{n-1} + s^n a_0 = 0.$$

Now pick any prime power p^k which divides r. Since the gcd of r and s is 1, from the last equation we see that p^k divides $s^n a_0$. Since the gcd of p^k and s^n is 1, p^k must divide a_0. Since this is true of all factors of r, r divides a_0. A similar argument shows that s divides a_n.

4. # 20 Suppose p is prime and $\Phi_p(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$. Show that Φ_p is irreducible over Q.

   Solution: No one asked me about this question so I assume everyone found the trick somewhere. We use Eisenstein applied to the polynomial $\Phi_p(x+1)$.

   $$\Phi_p(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = \sum_{k=1}^{p} \binom{p}{k} x^{k-1}.$$

   by the binomial theorem. The lead coefficient is 1 and all other coefficients are $\binom{p}{k}$ for $0 < k < p$. Since p is prime, p divides $\binom{p}{k}$ for $0 < k < p$ and since the constant term is $\binom{p}{1}$, p^2 does not divide it. So by Eisenstein, $\Phi_p(x+1)$ is irreducible over the rationals. But if Φ_p was reducible, say $\Phi_p = fg$ for polynomials f and g of lower degree then $\Phi_p(x+1) = f(x+1)g(x+1)$ and $f(x+1), g(x+1)$ still have lower degree than $\Phi_p(x+1)$ which contradicts its irreducibility over the rationals.

5. # 21 Show that for any field F, there are infinitely many irreducible polynomials over F in $F[x]$.

   Solutions: Ah, Euclid! Suppose that there are only finitely many polynomials $f_1, \ldots, f_n$ which are irreducible over F. Consider

   $$g = f_1 f_2 \ldots f_n + 1.$$

   If you divide g by f_i for any i then you will be left with a remainder of 1 so f_i does not divide g for any i. So if g is irreducible over F then it was not included in our list. If g is not irreducible then none of its irreducible factors was in our list. Either way, the original list did not contain all irreducible polynomials over F.

6. # 25 Define a function D on $F[x]$ as follows:

$D(a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0) = na_nx^{n-1}+(n-1)a_{n-1}x^{n2}+\ldots+a_1.$

(a) D is a homomorphism of abelian groups: Suppose that

$$f = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$$

and

$$g = b_mx^m + b_{m-1}x^{m-1} + \ldots + b_1x + b_0.$$

By adding 0's as coefficients, we can assume $m = n$ to make the notation simpler. Then

$$D(f + g) = n(a_n + b_n)x^{n-1]} + \ldots + (a_1 + b_1)$$

which equals

$$(na_nx^{n-1} + \ldots a_1) + (nb_nx^{n-1} + \ldots b_1)$$

which of course is $D(f) + D(g)$.

(b) If the characteristic of F is 0, the only polynomials in the kernel are the constant polynomials.

(c) if the characteristic of F is p then all polynomials of the form

$$a_nx^{pn} + \ldots + a_1x^p + a_0$$

for some n are in the kernel of D since $p = 0$ in F.

(d) Suppose that f and g are as above. The coefficient of x^k in fg is

$$\sum_{j=0}^{k} a_jb_{k-j}$$

and so the coefficient of x^{k-1} in $D(fg)$ is

$$k\sum_{j=0}^{k} a_jb_{k-j}.$$

On the other hand the coefficient of x^{k-1} in $D(f)g + fD(g)$ is

$$\sum_{j=0}^{k} ja_jb_{k-j} + \sum_{j=0}^{k}(k-j)a_jb_{k-j}$$

and if you bring these summations together, you see that $D(fg) = D(f)g + fD(g)$.

(e) Finally, suppose that f is a product of linear factors and some constant. We want to show that f has no multiple roots iff f and $D(f)$ have no common divisor. Assume that f has a multiple root. That would mean that we can write $f = (x-a)^2 g$ for some $a \in F$ and $g \in F[x]$. From what we have proved about the derivation, it follows that $D(f) = 2(x-a)g + (x-a)^2 D(g)$ and so $(x-a)$ is a common divisor of f and $D(f)$.

In the other direction, suppose that $f = u(x-a_1)\dots(x-a_n)$ with all the a_i's distinct. Then it follows that $D(f)$ is

$$u(x-a_2)\dots(x-a_n) + u(x-a_1)(x-a_3)\dots(x-a_n) \\ + \dots + u(x-a_1)\dots(x-x_{n-1})$$

where each term in the expression above is missing one of the linear factors. If f and $D(f)$ have a common divisor then they have a common linear divisor. Without loss we may assume that it is $(x-a_1)$. From the expression above, we see that $(x-a_1)$ divides all the terms of $D(f)$ except the first one. If we divide the first term by $(x-a_1)$, this is the same as evaluating it at a_1 and we get a remainder of

$$u(a_1-a_2)\dots(a_1-a_n).$$

Since all the a_i's are distinct this is not zero and so $(x-a_1)$ does not divide $D(f)$. We conclude that f and $D(f)$ have no common factors.