January 2013 Algebra Prelim

Sarah Arpin

1

Suppose $G = A \rtimes H$ is a finite group and A is abelian. Prove that the size of the conjugacy class of $a \in A$ in G is $|H : C_H(a)|$.

Solution:
The size of the conjugacy class of $a \in A$ in G is $|G : C_G(a)|$, so we want to show:

$$\frac{|G|}{|C_G(a)|} = \frac{|H|}{|C_H(a)|}$$

First, take $(b, h) \in C_G(a)$. Then:

$$\begin{aligned}
(b,h)(a,1) = (a,1)(b,h) &\Leftrightarrow (b(h \cdot a), h) = (ab, h) \\
&\Leftrightarrow b(h \cdot a) = ab \text{ and since } A \text{ is abelian:} \\
&\Leftrightarrow b(h \cdot a) = ba \\
&\Leftrightarrow h \cdot a = a \\
&\Leftrightarrow hah^{-1} = a \\
&\Leftrightarrow h \in C_H(a)
\end{aligned}$$

So an element of $C_G(a)$ does not depend on its first coordinate at all, it just depends on the second coordinate being in $C_H(a)$.
This means:

$$|C_G(a)| = |A| \cdot |C_H(a)|$$

Also note that since G is a semidirect product, $|G| = |A||H|$. Then, using this with the equation above:

$$\frac{|G|}{|C_G(a)|} = \frac{|G|}{|A||C_H(a)|}$$

$$\frac{|G|}{|C_G(a)|} = \frac{|A||H|}{|A||C_H(a)|}$$

$$\frac{|G|}{|C_G(a)|} = \frac{|H|}{|C_H(a)|}$$

Which establishes what we needed to show.

$\square$

2

Let $H, K \trianglelefteq G$, where G is a finite group.

(a) For each $P \in \mathrm{Syl}_p(HK)$, show that $P \cap H \in \mathrm{Syl}_p(H), P \cap K \in \mathrm{Syl}_p(K)$, and $P = (P \cap H)(P \cap K)$.

(b) Show that if H and K are nilpotent, then HK is nilpotent.

Solution:

(a) First, note that HK is a group, because we need at least one of H or K to be normal and they both are. Take $P \in \mathrm{Syl}_p(HK)$. Since H is a normal subgroup of G, P is in the normalizer of H and we can apply the Second Isomorphism Theorem:

$$HP/H \cong P/(P \cap H)$$

In terms of indices, this implies

$$|HP : H| = |P : P \cap H|$$

What we want to show is that $[H : P \cap H]$ is relatively prime to p. What we currently know is that $[G : P]$ is relatively prime to p.

$$\begin{aligned}
[G : P \cap H] &= [G : P \cap H] \\
[G : P][P : P \cap H] &= [G : H][H : P \cap H] \text{ by the 2nd Isom Thm:} \\
[G : P][HP : H] &= [G : H][H : P \cap H] \\
\left(\frac{|G|}{|P|}\right)\left(\frac{|HP|}{|H|}\right) &= \left(\frac{|G|}{|H|}\right)[H : P \cap H] \\
\left(\frac{|HP|}{|P|}\right) &= [H : P \cap H] \\
[HP : P] &= [H : P \cap H] \\
[HK : HP][HP : P] &= [H : P \cap H][HK : HP] \\
[HK : P] &= [H : P \cap H][HK : HP]
\end{aligned}$$

So $[H : P \cap H]$ is a factor of $[HK : P]$, which is relatively prime to p, and $[H : P \cap H]$ itself is thus also relatively prime to p. This means $P \cap H \in \mathrm{Syl}_p(H)$, as it is a maximal p-subgroup of H.
A symmetric proof establishes that $P \cap K \in \mathrm{Syl}_p(K)$.

3

Prove that the subring of $\mathbb{Q}[x]$ consisting of all polynomials with integer constant term is not a UFD.

Call the subring of $\mathbb{Q}[x]$ described R.
R is an integral domain, and its units are ± 1.
The irreducibles in R are $\pm p$ where p is a prime in $\mathbb{Z}$ and the polynomials $f(x) \in \mathbb{Q}[x]$ that are irreducible and have constant term ± 1.
Consider the element $x \in R$. x cannot be written as the product of irreducibles.
If it could, it would have at most one irreducible factor of the form $(ax \pm 1)$ where $a \in \mathbb{Q}$, because it is degree one. The other irreducible factors would have to be primes.
Consider one potential such factorization:

$$x = (ax \pm 1)p_1 ... p_n = ap_1 ... p_n x + p_1 ... p_n$$

But this would imply $p_1 ... p_n = 0$, which is not possible since these are nonzero elements of an integral domain R.
Thus, it is not possible to factor x into a product of irreducibles, so R is not a UFD.

$\square$

4

Does there exist a 6×6 matrix A

1. over $\mathbb{Q}$
2. over $\mathbb{R}$

such that $A^4 + I = A^2 - I$.

Solution:

1. If $A^4 + I = A^2 - I$, then $A^4 - A^2 + 2I = 0$, so the minimal polynomial of A must divide $x^4 - x^2 + 2$. We will show that the polynomial $x^4 - x^2 + 2$ is irreducible: if it were reducible, it would be reducible over $\mathbb{Z}_3[x]$, but when we consider the polynomial in $\mathbb{Z}_3[x]$:

   $$x^4 + 2x^2 + 2$$

   It does not have any linear factors:

   $$0^4 + 2(0^2) + 2 \neq 0$$
   $$1^4 + 2(1^2) + 2 \neq 0$$
   $$2^4 + 2(2^2) + 2 = 1 + 2 + 2 \neq 0$$

   It does not have any quadratic factors either, the only irreducible quadratics in $\mathbb{Z}_3[x]$ are $x^2 + 1$ and $x^2 + x + 1$ and:

   $$(x^2 + 1)^2 = x^4 + 2x^2 + 1$$
   $$(x^2 + x + 1)^2 = x^4 + 2x^3 + 2x + 1$$
   $$(x^2 + 1)(x^2 + x + 1) = x^4 + x^3 + 2x^2 + x + 1$$

   This establishes that $f(x) = x^4 - x^2 + 2$ is irreducible over $\mathbb{Q}$.
   Since $f(A) = 0$, the minimal polynomial must divide $f(x)$. Since $f(x)$ is irreducible, the minimal polynomial must be equal to $f(x)$.
   The minimal polynomial is the largest invariant factor of A, and all other invariant factors must divide the minimal polynomial, so in our case we see that the minimal polynomial is the only invariant factor of A.
   The characteristic polynomial is the product of all of the invariant factors of A, but this is then impossible, because the characteristic polynomial must have degree 6 and our only invariant factor is of degree 4. Thus, such a 6×6 matrix over $\mathbb{Q}$ cannot exist.

2.

5

How many roots does the polynomial $x^{2013} - 1$ have in the field $\mathbb{F}_{67}$? Note that $2013 = 3 \cdot 11 \cdot 61$.

Solution:
Since 0 is not a solution, the only solutions in $\mathbb{F}_{67}$ will be in $\mathbb{F}_{66}^{\times}$. This is a cyclic group, say it is generated by g. The order of g is 66.
If $x = g^k$ is a solution, then $x^{2013} - 1$, so $g^{2013k} = 1$. Then, the order of g must divide $2013k = 3 \cdot 11 \cdot 61 \cdot k$. 66 will divide $3 \cdot 11 \cdot 61 \cdot k$ if and only if k is an even number. There are 33 even powers of g in $\mathbb{F}_{66}^{\times}$, and these are exactly the roots $x^{2013} - 1$.

□

6

Let F be a field of characteristic 0. Show that if E/F is a normal field extension of prime degree p such that F contains the p^2ths roots of unity, then E has an extension of degree p.

Solution:
Since E/F is a normal field extension of prime degree p, E is the splitting field of some polynomial $f(x) \in F[x]$ where the degree of f is p.
All