August 2010 Algebra Prelim

Sarah Arpin

1

In this problem, you may assume without proof that the alternating groups A_n are simple for $n \geq 5$.

(a) Prove that any index 6 subgroup of the alternating group A_6 is isomorphic to A_5.

(b) Show that any simple group of order 60 is isomorphic to A_5.

Solution:

(a) Let $H \leq A_6$ such that $|A_6 : H| = 6$.
Let $S = \{H, \sigma_1 H, \sigma_2 H, ..., \sigma_5 H\}$ denote the 6 distinct left cosets of H in A_6.
Let A_6 act on the cosets in S by left multiplication.
The stabilizer of this action on H is equal to H:

$$\begin{aligned} x \in \mathrm{Stab}_G(H) &\Leftrightarrow xH = H \\ &\Leftrightarrow x \in H \end{aligned}$$

The elements in $\mathrm{Stab}_G(H)$ fix H, so they must permute the other 5 cosets of H. Thus, $\mathrm{Stab}_G(H) \leq A_5$, and thus $H \leq A_5$.
Also, $|H| = 60 = |A_5|$, so this means $H \cong A_5$.

(b) Let G be a simple group of order $60 = 2^2 \cdot 3 \cdot 5$.
By the Sylow theorems, $n_5 \equiv 1 \pmod 5$, and $n_5 | 2^2 \cdot 3 = 12$, so $n_5 = 6$, since $n_5 \neq 1$ when G is simple.
Let G act on the Sylow 5-subgroups by conjugation. This action induces an injective homomorphism φ of G into S_6.
$\varphi(G) \cap A_6 \neq 0$, because $\varphi(G)$ cannot contain only odd permutations. Thus $\varphi^{-1}(A_6)$ must be a normal subgroup of G, so it must be all of G. Thus, $\varphi(G)$ is a subgroup of A_6. Since φ is injective, $|G| = |\varphi(G)|$, so $|A_6 : G| = 6$, and we can apply the result from part (a).

□

2

Let G be a finite group with a normal subgroup $N \trianglelefteq G$, and suppose $\theta : G \to H$ is a group homomorphism into a solvable group H. Show that if the commutator subgroup of G/N is itself, then $\theta(G) = \theta(N)$.

Solution:
Consider the induced map $\overline{\theta} : G/N \to \theta(G)/\theta(N)$ defined via $\overline{\theta}(gN) = \theta(g)\theta(N)$.
Consider the following:

$$\begin{aligned}\theta(G)/\theta(N) &= \overline{\theta}(G/N) \\ &= \overline{\theta}([G/N, G/N]) \\ &= [\overline{\theta}(G/N), \overline{\theta}(G/N)] \\ &= [\theta(G)/\theta(N), \theta(G), \theta(N)]\end{aligned}$$

So $\theta(G)/\theta(N) = [\theta(G)/\theta(N), \theta(G), \theta(N)]$. This means that the derived series of $\theta(G)/\theta(N)$ is just $\theta(G)/\theta(N)$.
Since $\theta(G) \leq H$ and H is solvable, $\theta(G)$ is solvable.
Quotients of solvable groups are also solvable, so $\theta(G)/\theta(N)$ must also be solvable.
If $\theta(G)/\theta(N)$ is solvable, its derived series must eventually be 1, but we showed that its derived series is just $\theta(G)/\theta(N)$, so this means

$$\theta(G)/\theta(N) = 1$$

Which implies $\theta(G) = \theta(N)$, as desired.

□

3

Show that x, y, and z are irreducible and prime elements of $k[x, y, z]$, where k is a field. Prove that $k[x, y, z]/\langle xy - z^2 \rangle$ is an integral domain.

Solution:
First, consider the ideal (x). x is prime if and only if $k[x, y, z]/(x)$ is an integral domain. However, $k[x, y, z]/(x) \cong k[y, z]$, which we know is an integral domain since it is a polynomial extension of a field. Thus, (x) must be a prime ideal. In an integral domain, every prime is irreducible, so x must be prime and irreducible. This holds for the other indeterminates as well.
To show that $R = k[x, y, z]/\langle xy - z^2 \rangle$ is an integral domain, consider the elements of R, noting that $xy = z^2$.

$$\begin{aligned}
\sum_{i,j,k \in \mathbb{N} \cup \{0\}} x^i y^j z^k &= \sum_{i \geq j, k \in \mathbb{N} \cup \{0\}} x^i y^j z^k + \sum_{i < j, k \in \mathbb{N} \cup \{0\}} x^i y^j z^k \\
&= \sum_{i \geq j, k \in \mathbb{N} \cup \{0\}} (xy)^j x^{i-j} z^k + \sum_{i < j, k \in \mathbb{N} \cup \{0\}} (xy)^i y^{j-i} z^k \\
&= \sum_{i \geq j, k \in \mathbb{N} \cup \{0\}} x^{i-j} z^{k+2j} + \sum_{i < j, k \in \mathbb{N} \cup \{0\}} y^{j-i} z^{k+2i} \\
&\in k[x, z] + k[y, z]
\end{aligned}$$

$k[x, z]$ and $k[y, z]$ are both integral domains, so its sum must be as well.
Thus, none of these elements can be zero divisors so R is an integral domain.

□

4

Let p be an odd prime, and let $SL_2(\mathbb{F}_p)$ be the group of all 2×2 matrices with determinant 1 over $\mathbb{F}_p$. Show that $SL_2(\mathbb{F}_p)$ has $p+2$ conjugacy classes.

Solution:
The distinct conjugacy classes will have distinct rational canonical forms, so we need to count the possible rational canonical forms of the matrices in $SL_2(\mathbb{F}_p)$. To count these, we can count the number of possible minimal polynomials of matrices in $SL_2(\mathbb{F}_p)$.
Consider an arbitrary matrix $A \in SL_2(\mathbb{F}_p)$ and calculate its characteristic polynomial:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : ad - bc = 1$$

The characteristic polynomial can be calculated by finding the determinant of $\lambda I - A$:

$$\begin{aligned} c_A(x) &= \det(\lambda I - A) \\ &= (\lambda - a)(\lambda - d) - bc \\ &= \lambda^2 - (a+d)\lambda + ad - (ad - 1) \\ &= \lambda^2 - (a+d)\lambda + 1 \end{aligned}$$

The number of possible characteristic polynomials of this form is p.
If $c_A(x)$ splits into distinct linear factors, then the minimal polynomial must be equal to the characteristic polynomial, and we only have one option for minimal polynomials of this form. This is because the minimal polynomial must divide the characteristic polynomial and it must have the same roots.
If there is a double root, then $c_A(x)$ must be of the form $(x+1)^2$ or $(x-1)^2$, because the only square roots of 1 in $\mathbb{F}_p$ are 1 and -1.
If $c_A(x) = (x-1)^2$, then there is one more possibility for $m_A(x)$ aside from $m_A(x) = c_A(x)$, namely: $m_A(x) = (x-1)$. Likewise for the situation where $c_A(x) = (x+1)^2$.
Thus, we add two more possiblities to the list of minimal polynomials, so the number of possible minimal polynomials is $p+2$.
As discussed above, this means the number of possible conjugates in $SL_2(\mathbb{F}_p)$ is $p+2$.

□

5

No.

6

Let $E = \mathbb{F}_{2^5}$ be the field with 32 elements, let $F = \mathbb{F}_2$ be the prime subfield of E, let A be an algebraic closure of E, and let c be a root in A of $f(x) = x^4 + x^3 + 1$ in $\mathbb{F}[x]$.

(a) Show that $f(x)$ is irreducible in $F[x]$.

(b) Find the splitting field of $f(x)$, regarded as a polynomial in $E[x]$.

Solution:

1. First, check to see if $f(x)$ has linear factors by plugging in the elements of $\mathbb{F}$:

$$f(0) = 1 \neq 0$$

$$f(1) = 1 + 1 + 1 = 1 \neq 0$$

So $f(x)$ has no linear factors.
Next, consider the possibility that $f(x)$ has quadratic factors. They would necessarily be irreducible, because $f(x)$ does not have linear factors.
The only irreducible quadratic in $\mathbb{F}$ is: x^2+x+1, because $x^2+1 = (x+1)(x+1)$ and $x^2+x = x(x+1)$.

$$(x^2 + x + 1)(x^2 + x + 1) = x^4 + 2x^3 + 3x^2 + 2x + 1 = x^4 + x^2 + 1 \neq f(x)$$

So $f(x)$ does not have quadratic factors either. Thus, $f(x)$ is irreducible in $\mathbb{F}$.

2. Since $f(x)$ is irreducible in $\mathbb{F} = \mathbb{F}_2$ and the degree of f is 4, $f(x)$ split in $\mathbb{F}_{2^4}$. The smallest field containing both $\mathbb{F}_{2^5} = E$ and $\mathbb{F}_{2^4}$ is $\mathbb{F}_{2^20}$, so this the splitting field of $f(x)$ as a polynomial over E.

□