August 2016 Algebra Prelim

Sarah Arpin

1

Prove that, up to isomorphism, there is a unique group of order 1001 ($= 7 \times 11 \times 13$).

Solution 1:
If $|G|$ and $\varphi(|G|)$ are relatively prime, then there is a unique group of order $|G|$.

$$\varphi(1001) = 6 \times 10 \times 12 = 720$$

$$\gcd(1001, 720) = 1$$

Thus, there is a unique group of order 1001, namely $\mathbb{Z}_{1001}$.

Solution 2:
If G is abelian, then the only invariant factor of 1001 is 1001, since it is a product of distinct primes, so by the Fundamental Theorem of Finitely Generated Abelian Groups $G \cong \mathbb{Z}_{1001}$.
It remains to show that there are no non-abelian groups of order 1001.
Consider the Sylow numbers of G, by the Sylow theorems:

- n_7 must be congruent to 1 mod 7, and it must divide $11 \cdot 13$. The only possibility is $n_7 = 1$, which makes the Sylow 7-subgroup of G unique and thus normal. (If there's only one Sylow p-subgroup P of a group G, any conjugates gPg^{-1} are also Sylow p-subgroups, so $P = gPg^{-1}$, making P normal.)
- n_{11} must be congruent to 1 mod 11, and it must divide $7 \cdot 13$. The only possibility is $n_{11} = 1$, which makes the Sylow 11-subgroup of G unique and thus normal.
- n_{13} must be congruent to 1 mod 13, and it must divide $7 \cdot 11$. The only possibility is $n_{13} = 1$, which makes the Sylow 13-subgroup of G unique and thus normal.

If the order of a group is pq, where p, q are primes with $p \nmid (q-1)$, then the group is abelian.
If G' denotes the commutator subgroup of G, then G/G' is the largest abelian quotient of G: If $H \trianglelefteq G$ and G/H is abelian, then $G' \leq H$.
Let P_7, P_{11}, P_{13} denote the Sylow 7-,11-, and 13-subgroups of G, respectively.

- $|G/P_7| = 11 \cdot 13$, so G/P_7 is abelian and $G' \leq P_7$.
- $|G/P_{11}| = 7 \cdot 13$, so G/P_{11} is abelian and $G' \leq P_{11}$.
- $|G/P_{13}| = 7 \cdot 11$, so G/P_{13} is abelian and $G' \leq P_{13}$.

Since G' is a subgroup of each Sylow p-subgroup of G, it must be in the intersection of these Sylow p-subgroups of G. But the distinct Sylow p-subgroups of G intersect only in the identity, so $G' = \{e\}$, which means G is abelian, as $x^{-1}y^{-1}xy = 1$ for all $x, y \in G$.

□

2

Let S_n be the symmetric group on n symbols.

(i) Prove that if $2 \leq n \leq 4$ then there is a surjective homomorphism of groups from S_n to S_{n-1}.

(ii) Prove that if $n \geq 5$ then there is no surjective homomorphism of groups from S_n to S_{n-1}.

Solution:

(i) Take the cases $n = 2, 3, 4$ separately.

- If $n = 2$, then define $\varphi : S_2 \to S_1$ via $\varphi(x) = 1$. This is a surjective homomorphism since $\varphi(x)\varphi(y) = 1 \cdot 1 = 1 = \varphi(xy)$.
- If $n = 3$, then define $\varphi : S_3 \to S_2$ via:

$$\varphi(x) = \begin{cases} (1) & \text{if } x \text{ is even} \\ (12) & \text{if } x \text{ is odd} \end{cases}$$

  This is surjective, since S_3 contains both even and odd permutations.
  This is a homomorphism, since the product of two even permutations is even, the product of two odd permutations is even and $(12)(12) = (1)$, and the product of an even and an odd permutation is odd.
- If $n = 4$, consider the subgroup $K \leq S_4$:

$$K = \{(1), (12)(34), (13)(24), (14)(23)\}$$

  S_4 acts on the nonidentity elements of K by conjugation and permutes them. This action is nontrivial:

$$(12)(12)(34)(12) = (14)(23)$$
$$(12)(13)(24)(12) = (12)(34)$$
$$(12)(14)(23)(12) = (13)(24)$$

  This action gives a homomorphism taking each of the elements of S_4 to a permutation on 3 elements, so mapping S_4 to S_3.

(ii) By contradiction, suppose that there is a surjective homomorphism $\varphi : S_n \to S_{n-1}$, $|\varphi(S_n)| = (n-1)!$.
By the first isomorphism theorem, $S_n/\ker\varphi \cong S_{n-1}$.
By Lagrange, $|\ker\varphi| = n$, $n \geq 5$.
The kernel is always a normal subgroup, so $\ker\varphi \trianglelefteq S_n$.
We know that for $n \geq 5$, A_n is simple, so if we can show that the kernel has nontrivial intersection with A_n, we will show the kernel has to be trivial.
$|A_n| = n!/2 \neq n$,since $n \geq 5$, so $\ker\varphi \neq A_n$. However, $\ker\varphi$ cannot contain only odd permutations, since the product of two odd permutations is even, so $\ker\varphi \cap A_n$ is nontrivial. But since $\ker\varphi$ is normal in S_n, the intersection $\ker\varphi \cap A_n$ will be normal in A_n, but A_n is simple and has no nontrivial normal subgroups. This leads to a contradiction, so no such homomorphism φ is possible.

□

3

Let R be a commutative ring with identity.

(i) Suppose I is an ideal of R that is contained in the principal ideal $\langle a \rangle$. Show that there is an ideal J of R such that $I = \langle a \rangle J$.

(ii) Suppose $R = \mathbb{C}[x, y]$. Give an example of two ideal $I \subseteq A$ of R for which there is no ideal J satisfying $I = AJ$.

Solution:

(i) Let $J = \{r \in R : \langle a \rangle r \subseteq I\}$
J is an ideal of R, because if $x \in R$ and $r \in J$, then $\langle a \rangle r \subseteq I \Rightarrow \langle a \rangle xr \subseteq I$, so $xr \in J$.
By construction $\langle a \rangle J \subseteq I$. To show the two ideals are equal, show containment in the other direction.
Since $I \subseteq \langle a \rangle$, every element of I is of the form ar, for some $r \in R$.
For any $r' \in R$, $arr' \in I$, since I is an ideal.
R is commutative, so $ar'r \in I$ for all $r' \in R$. Then, $\langle a \rangle r \subseteq I$, so $r \in J$, $ar \in \langle a \rangle J$, and we have $I \subseteq \langle a \rangle J$.
Since inclusion holds in both directions, $I = \langle a \rangle J$.

(ii) Let $A = \mathbb{C}[x, y]$, and let $I = \langle x \rangle$. There is no ideal J for which $I = AJ$. For example $x + y \in A$, but there is no $r \in \mathbb{C}[x, y]$ such that $(x + y)r \in \langle x \rangle$.

□

4

Let F be a field and let $A \in M_n(F)$ be a non-invertible $n \times n$ matrix over F.

1. Prove that if 0 is the only eigenvalue of A in F, and F is algebraically closed, then we have $A^n = 0$.
2. Find an example of a field F and a noninvertible matrix $A \in M_n(F)$ such that 0 is the only eigenvalue of A in F, but such that we do not have $A^n = 0$.

Solution:

1. If F is algebraically closed and 0 is the only eigenvalue of A in F, then 0 is the only eigenvalue of A, period.
   Consider the Jordan Canonical Form of A: A is similar to an $n \times n$ matrix $P^{-1}AP$, which is in Jordan canonical form, i.e., $P^{-1}AP$ is a block diagonal matrix whose diagonal blocks are the Jordan blocks of the elementary divisors of A. This means that A is similar to a matrix which is strictly upper triangular. A strictly upper triangular matrix is necessarily nilpotent, so A is nilpotent, and $A^n = 0$.
2. Let $F = \mathbb{R}$ (which is a field, but is not algebraically closed) and consider the matrix A:

$$A = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}$$

   The only eigenvalue of A is 0, because its characteristic polynomial is $c(\lambda) = \lambda(\lambda^2 + 1)$:

$$c(\lambda) = \det(I\lambda - A) = \begin{vmatrix} \lambda & 0 & 0 \\ 0 & \lambda & -1 \\ 0 & 1 & \lambda \end{vmatrix} = \lambda \begin{vmatrix} \lambda & -1 \\ 1 & \lambda \end{vmatrix} = \lambda(\lambda^2 + 1)$$

   The only zero of $c(\lambda)$ in F is 0.

   Now, show $A^3 \neq 0$:
   When we multiply A by itself, we swap the second and third rows, then negate the third row. This will never give us 0, and certainly does not give us $A^3 = 0$:

$$A^2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \; A^3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}$$

   Another way to show $A^3 \neq 0$ is to look at the characteristic polynomial of A. By Cayley-Hamilton, A satisfies its own characteristic polynomial:

$$c(A) = 0 \Rightarrow A^3 + A = 0 \Rightarrow A^3 = -A \neq 0$$

5

Let L/K be a Galois extension of fields. The *norm* map from L to K is defined to be

$$N(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha)$$

(i) Show that N restricts to a homomorphism of groups from L^* to K^*.

(ii) Let $\mathbb{F}_q$ denote the field with q elements and let m be a positive integer. Show that $N : \mathbb{F}_{q^m}^* \to F_q^*$ is surjective. [Hint: use the Frobenius automorphism.]

(iii) Let σ be a generator for $\mathrm{Gal}(F_{q^m}/F_q)$. Compute the cardinality of

$$S = \left\{ \frac{\alpha}{\sigma(\alpha)} : \alpha \in \mathbb{F}_{q^m}^* \right\}$$

(iv) Show that $\ker(N) = S$, where N and S are as defined in parts (ii) and (iii) respectively.

Solution:

(i) Consider $N(1)$:

$$N(1) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(1) = 1$$

Since all of the σ are homomorphisms, $\sigma(1) = 1$.
Since N is multiplicative, $N : L^\times \to K^\times$ is a group homomorphism.

Table 1: Galois Group: Actions of Automorphisms on Roots

Automorphism	Effect on ξ	Effect on i
1	ξ	i
σ	$i\xi$	i
σ^2	$-\xi$	i
σ^3	$-i\xi$	i
τ	ξ	$-i$
$\sigma\tau$	$i\xi$	$-i$
$\sigma^2\tau$	$-\xi$	$-i$
$\sigma^3\tau$	$-i\xi$	$-i$

6

Let $f = x^4 - 3$. Find the degree of the splitting field of f over $\mathbb{Q}$. Describe the Galois group of f, by giving its action on the roots of f explicitly, and identifying it as isomorphic to a known finite group.

Solution:
f factors:

$$f(x) = (x - \xi)(x + \xi)(x - i\xi)(x + i\xi)$$

where $\xi = \sqrt[4]{3}$.
The splitting field of f is $\mathbb{Q}[\xi, i]$. The extension $\mathbb{Q}[\xi, i] : \mathbb{Q}$ is finite and normal, because $\mathbb{Q}[\xi, i]$ is a splitting field for the polynomial f.
By Eisenstein's criterion, f is irreducible: Consider the prime $p = 3$: $3 \nmid a_4 = 1$, $3 \mid a_3, a_2, a_1 = 0$, and $3 \mid a_0 = 3$, $3^2 \nmid a_0 = 3$. Thus, f satisfies Eisenstein's criteria for irreducibility.
To find the degree of the extension $\mathbb{Q}[\xi, i] : \mathbb{Q}$, consider the tower law:

$$[\mathbb{Q}[\xi, i] : \mathbb{Q}] = [\mathbb{Q}[\xi, i] : \mathbb{Q}[\xi]] \cdot [\mathbb{Q}[\xi] : \mathbb{Q}]$$

The minimal polynomial of ξ over $\mathbb{Q}$ is f, because $f(\xi) = 0$ and f is irreducible, so $[\mathbb{Q}[xi] : \mathbb{Q}] = 4$.
The minimal polynomial of i over $\mathbb{Q}[\xi]$ is $x^2 + 1$, so $[\mathbb{Q}[\xi, i] : \mathbb{Q}[\xi]] = 2$.
By the tower law, this means $[\mathbb{Q}[\xi, i] : \mathbb{Q}] = 8$.
To find the elements of the Galois group of $\mathbb{Q}[\xi, i] : \mathbb{Q}$, we need to find the automorphisms of $\mathbb{Q}[\xi, i]$ that fix $\mathbb{Q}$.
Consider the automorphisms σ, τ given:

$$\sigma(i) = i, \sigma(\xi) = i\xi, \tau(i) = -i, \tau(\xi) = \xi$$

σ and τ will generate the Galois group, which we know is order 8. Consider the relations in Table 1.
The Galois group is generated by an element of order 4 and an element of order 2, so it is isomorphic to $\mathbb{D}_8$.