Kayla Orlinsky

Algebra Exam Fall 2013

Problem 1. Let H be a subgroup of the symmetric group S_5. Can the order of H be $15, 20$ or 30?

Solution. First, S_5 does have a subgroup of order 20. Since by Sylow, $n_5 \equiv 1 \mod 5$ and $n_5 | 24$, $n_5 = 1, 6$. Since S_5 has no normal subgroups other than A_5, $n_5 = 6$. Therefore, by Sylow, $[S_5 : N_{S_5}(P_5)] = n_5 = 6$ where P_5 is a Sylow 5-subgroup of S_5.

Therefore, $N_{S_5}(P_5)$ is a subgroup of S_5 of order $120/6 = 20$.

To disprove the other subgroups, we prove a claim.

Claim 1. For $n \geq 5$, there are no subgroups of S_n with $2 < [S_n : H] < n$.

Proof. Note that A_n is always a subgroup of S_n of index 2.

Let H be a subgroup of S_n such that $2 < [S_n : H] = k < n$. Let S_n act on $X = S_n/H$ the set of left cosets of H by left-multiplication.

Then because $2 < |X| < n$, this induces a homomorphism from S_n to S_k where $k = |X|$.

Specifically, this defines a map

$$\varphi : S_n \to S_{|X|} = S_k$$
$$a \mapsto \sigma_a$$

where $\sigma_a : X \to X$ is defined by $\sigma_a(bH) = abH$.

Now, we note that if a is in the kernel of this homomorphism, then $abH = bH$ for all $b \in S_n$ and so namely, $abh = bh'$ for $h, h' \in H$ so $a = bh'h^{-1}b^{-1} \in bHb^{-1}$.

Thus, $a \in bHb^{-1}$ for all $b \in S_n$ and so $a \in eHe^{-1} = H$.

Therefore, $\ker(\varphi) \subset H$.

Finally, we note that for $n \geq 5$, the only normal subgroups of S_n are the trivial subgroup, S_n itself, and A_n. Since $[S_n : A_n] = 2 < [S_n : H] < n$, $\ker(\varphi) \neq S_n$ and not A_n.

Namely, the kernel is trivial and so we have an embedding of S_n into a symmetric group of strictly smaller degree, which is of course, nonsense.

Thus, H cannot exist. ✌

By the claim, since $|S_5| = 120$, If $|H| = 30$ then $[S_5 : H] = 120/30 = 4 < 5$, so there are no subgroups of order 30.

If H had a subgroup of order 15 and P_2 was a sylow 2-subgroup of S_5, then

$$|HP_2| = \frac{|H||P_2|}{|H \cap P_2|} = \frac{15 \cdot 8}{1} = 120 = |G|$$

it must be that $S_5 = HP_2$.

Now, in H, by Sylow $n_5|3$ and $n_5 \equiv 1 \mod 5$, so $n_5 = 1$, and $n_3 \equiv 1 \mod 3$ and $n_3|5$ so $n_3 = 1$. Thus H has a normal Sylow 3 and Sylow 5-subgroup, namely H is normal, since the product of two normal subgroups is normal.

However, S_5 has no normal non-trivial subgroups other than A_5 which has order 60. Namely, this is not possible. ✌

Problem 2. Let R be a PID and M a finitely generated torsion module of R. Show that M is a cyclic R-module if and only if for any prime $\mathfrak{p}$ of R either $\mathfrak{p}M = M$ or $M/\mathfrak{p}M$ is a cyclic R-module.

Solution.

$\boxed{\Longrightarrow}$ Assume M is cyclic. Then $M = (x) = xR = \{rx \mid r \in R\}$ for some $x \in X$. However, then M/PM is certainly cyclic since any quotient of a cyclic module must also be cyclic.

This is because we can define $\pi : M \to M/PM$ to be the quotient map, which is surjective. Then $M/PM \cong \pi((x)) = (\pi(x))$ and so is cyclic.

***Note that quotiens of cyclic modules are cyclic always. M need not be torsion for this to be true.

$\boxed{\Longleftarrow}$ Assume $PM = M$ or M/PM is cyclic for all *nonzero* prime ideals P.

By the structure theorem, there is a chain of ideals

$$(d_1) \subset (d_2) \subset \cdots \subset (d_n)$$

such that

$$M \cong R/(d_1) \oplus \cdots \oplus R/(d_n).$$

Note that $d_i | d_{i-1}$ for all i.

If (d_n) is not maximal, then there is a maximal (prime) ideal P such that $(d_n) \subset P$.

Then if $PM = P/(d_1) \oplus \cdots \oplus P/(d_n) = M$ we have that $P/(d_i) \cong R/(d_i)$ for all i, so $P = R$ which is a contradiction.

Thus, M/PM is cyclic so

$$M/PM \cong (R/(d_1))/(P/(d_1)) \oplus \cdots \oplus (R/(d_n))/(P/(d_n)) \cong (R/P)^n$$

However, M/PM is cyclic and $(R/P)^n \cong R/(a)$ for some a forces $n = 1$. Namely, M is cyclic.

***Note that torsion is not a necessary condition, only finitely generated is necessary for the backward implication.

✌

Problem 3. Let $R = \mathbb{C}[x_1, ..., x_n]$ and suppose I is a proper non-zero ideal of R. The coefficients of a matrix $A \in M_n(R)$ are polynomials in $x_1, ..., x_n$ and can be evaluated at $\beta \in \mathbb{C}^n$; write $A(\beta) \in M_n(\mathbb{C})$ for the matrix so obtained. If for some $A \in M_n(R)$ and all $\alpha \in Var(I)$, $A(\alpha) = 0_{n\times n}$, show that for some integer m, $A^m \in M_n(I)$.

Solution. By Nullstellensatz, if $A(\alpha) = 0$ for all $\alpha \in V(I)$, then every polynomial in every entry of A is in $\sqrt{I}$. Namely, if f_{ij} is the polynomial in the $(A)_{ij}$ entry, then $f_{ij} \in \sqrt{I}$ so there exists m_{ij} so $f_{ij}^{m_{ij}} \in I$.

Let $m = \text{lcm}\{m_{ij}\}$. Then the entries of A^{n^2} are sum of products of n^2 of the f_{ij}. Namely, $A^{n^2 m}$ will be a sum of products where at least one of the f_{ij} is raised to the power m, and so namely, that whole product is in I because I is a 2-sided (because R is commutative) ideal.

Thus, $A^{n^2 m} \in M_n(I)$. ✌

Problem 4. If R is a noetherian unital ring, show that the power series ring $R[[x]]$ is also a noetherian unital ring.

Solution. We will show that every ideal of $R[[x]]$ is finitely generated. Note that a formal power series $f(x)$ is invertible if and only if its constant term is a unit. Namely, $R[[x]]$ has a unit.

Now, let I be an ideal of $R[[x]]$.

Then, let

$$I_n = \{a \in R \,|\, ax^n + \text{ higher order terms } \in I\}.$$

Then I_n is an ideal of R since I is an ideal of $R[[x]]$

Then we have an increasing chain

$$I_0 \subset I_1 \subset I_2 \subset \cdots$$

since if $a \in I_n$, then $ax^n + bx^{n+1} + \cdots \in I$, so $x(ax^n + bx^{n+1} + \cdots) \in I$ so $(ax^{n+1} + bx^{n+2} + \cdots) \in I$ because I is a left ideal. Therefore, $a \in I_{n+1}$ so $I_n \subset I_{n+1}$.

Finally, the chain must terminate since R is noetherian, and so $I_m = I_n$ for all $m \geq n$, some n. Thus, if $ax^{n+1} + \cdots \in I$ then $ax^n + \cdots \in I$.

Now, because R is noetherian, all ideals are finitely generated and so let $I_i = (a_1^{(i)}, a_2^{(i)}, ..., a_{n_i}^{(i)})$ for $i = 0, ..., n$. Note that we can let $m = \max\{n_i\}$ and then write

$$I_i = (a_1^{(i)}, a_2^{(i)}, ..., a_m^{(i)}) \qquad a_j^{(i)} = 0 \forall j > n_i.$$

By definition of the I_i, there exist the following set of polynomials in I

$$F = \begin{bmatrix} a_1^{(0)} + \cdots & a_2^{(0)} + \cdots & \cdots & a_m^{(0)} + \cdots \\ a_1^{(1)}x + \cdots & a_2^{(1)}x + \cdots & \cdots & a_m^{(1)}x + \cdots \\ & \vdots & \ddots & \vdots \\ a_1^{(n)}x^n + \cdots & a_2^{(n)}x^n + \cdots & \cdots & a_m^{(n)}x^n + \cdots \end{bmatrix}$$

Then, if $f_{i,j} = (F)_{i,j}$ we have that $f_{i,j} \in I$ for all i, j.

Finally, let $f \in I$. Let $f(x) = \sum_{i=0}^{\infty} \alpha_i x^i$.

Then, α_j is a linear combination of the $a_i^{(j)}$ because they are exactly the generators of I_j. Therefore, we can write the first n-terms of f using the $f_{i,j}$, namely,

$$f(x) - \sum_{i=0}^{n}\sum_{j=1}^{m} b_j^{(i)} f_{i,j} = \alpha'_{n+1}x^{n+1} + \cdots \qquad b_j^{(i)} \in R.$$

Namely, $\alpha'_{n+1} \in I_{n+1} = I_n$ because the chain terminates at n.

Thus, we can write the next $n+1$ terms in the sequence in terms of the $f_{n,j}$. Specifically,

$$f(x) - \sum_{i=0}^{n}\sum_{j=1}^{m} b_j^{(i)} f_{i,j} - x^{n+1}\sum_{j=1}^{n} b_j^{(n)} f_{n,j} = \alpha''_{2n+2}x^{2n+2} + \cdots$$

Since the next $n+1$ block can again be generated by the $f_{n,j}$ for $j = 1, ..., m$ we finally have by grouping, that

$$f(x) = \sum_{i=0}^{n}\sum_{j=1}^{m} b_j^{(i)} f_{i,j} + \left(\sum_{k=0}^{\infty} c_k x^{k(n+1)}\right) f_{n,1} + \cdots + \left(\sum_{k=0}^{\infty} c'_k x^{k(n+1)}\right) f_{n,m}$$

and so at last,

$$I = (f_{i,j})_{i=0,..,n,j=1,...,m}$$

and is finitely generated.

Thus, $R[[x]]$ is noetherian since all its ideals are finitely generated.

✌

Problem 5. Let p be a prime. Prove that $f(x) = x^p - x - 1$ is irreducible over $\mathbb{Z}/p\mathbb{Z}$. What is the Galois group? (Hint: observe that if α is a root of $f(x)$, then so is $\alpha + i$ for $i \in \mathbb{Z}/p\mathbb{Z}$.)

Solution. First, note that $\mathbb{Z}_p \cong \mathbb{F}_p$. Let α be a root of f in the algebraic closure of $\mathbb{F}_p$. Then $f(\alpha) = \alpha^p - \alpha - 1 = 0$ so $\alpha^p - \alpha = 1$. Since

$$f(\alpha + i) = (\alpha + i)^p - (\alpha + i) - 1 = \alpha^p + i^p - \alpha - i - 1 = \alpha^p - \alpha - 1 = f(\alpha) = 0$$

since $i^p = i$ for all $i \in \mathbb{F}_p$.

Thus, f has p roots of the form, $\alpha, \alpha + 1, ..., \alpha + (p - 1)$.

Assume $f(x) = g(x)h(x)$ for $g, h \in \mathbb{F}_p[x]$ where g is the minimal polynomial of α (so g is irreducible and has α as a root). Then because $\alpha \notin \mathbb{F}_p$, g has at least one other $\alpha + i$ as a root. Therefore,

$$f(x + i) = g(x + i)h(x + i) = f(x) = g(x)h(x).$$

Thus, $g(x+i)$ is monic and also irreducible and also has α as a root, and so $g(x) = g(x+i)$. However, then the permutation $x \mapsto x + i$ preserves the roots of g, so g has the same roots as f and so $g = f$.

Thus, f is irreducible.

Finally, let $L = \mathbb{F}_p(\alpha)$. Then L is the splitting field for a separable polynomial and so $L/\mathbb{F}_p$ is Galois.

Clearly $[L : \mathbb{F}_p] = p$ and $G = \text{Gal}(L/\mathbb{F}_p)$ is generated by $\alpha \mapsto \alpha + 1$. Thus, $G \cong \mathbb{Z}_p$. ✌

Problem 6. Let R be a finite ring with no nilpotent elements. Show that R is a direct product of fields.

Solution. Since R is finite, it is necessarily artinian.

Let $x \in J(R)$. Then because $J(R)$ is right quasi-regular, $1 - x$ is a unit in R.

Then, we construct a decreasing chain of ideals

$$(x) \supset (x^2) \supset \cdots$$

which must terminate for some n. Namely, $(x^n) = (x^{n+1})$ so $x^n = rx^{n+1}$ for some $r \in R$. However, $rx \in J(R)$ and so $1 - rx$ is a unit. Therefore,

$$x^n = rx^{n+1} \implies x^n(1 - rx) = 0 \implies x^n = 0.$$

Namely, x is nilpotent. Since R has no nilpotent elements, $J(R) = 0$.

Thus, by Artin Wedderburn,

$$R \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_k}(D_k)$$

where the D_k are division rings.

Now, R contains no nilpotent elements, however matrix rings contain nilpotent elements over any division ring, since

$$\begin{bmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 0 & 0 \\ & \vdots & \ddots & \vdots & \\ 0 & 0 & \cdots & 0 & 0 \end{bmatrix}$$

is nilpotent of degree 2 over any division ring where $1 \neq 0$.

Namely, $n_i = 1$ for all i.

Finally, because the D_i are finite, by Wedderburn, the D_i are all fields.

Thus, R is a finite direct sum (isomorphic to a finite direct product) of fields. ✌

Problem 7. Let $K \subset \mathbb{C}$ be the field obtained by adjoining all roots of unity in $\mathbb{C}$ to $\mathbb{Q}$. Suppose $p_1 < p_2$ are primes, $a \in \mathbb{C} \backslash K$, and write L for a splitting field of

$$g(x) = (x^{p_1} - a)(x^{p_2} - a)$$

over K. Assuming each factor of $g(x)$ is irreducible, determine the order and the structure of $\mathrm{Gal}(L/K)$.

Solution. First, $g(x)$ is not a polynomial in $K[x]$, since $a \notin K$. However, if we assume that $a \in \mathbb{Q}$ is such that each factor of $g(x)$ is irreducible, then we do have that $g \in K[x]$.

Then, since L is the splitting field of a separable polynomial (since each factor of g is irreducible over $\mathbb{Q}$, it is separable), we have that L/K is Galois.

Furthermore, each $\sigma \in G = \mathrm{Gal}(L/K)$ will be uniquely determined by how it permutes the roots of each irreducible factor.

Namely, G will be generated by the σ_i, where σ_i is a permutation of the roots of $x^{p_i} - y$, fixing the other roots of g.

This implies that G will be abelian since each σ_i will fix all but the p_i^{th} roots of unity and will fix all p_i^{th} roots of y.

Therefore,

$$G \cong \mathbb{Z}_{p_1 p_2}.$$

✌