Kayla Orlinsky

Algebra Exam Fall 2010

Problem 1. Use Sylow's Theorems to show that any group of order $(99^2 - 4)^3$ is solvable.

Solution. First, we decompose the number.

$$\begin{aligned}
99^2 - 4 &= (100-1)^2 - 4 \\
&= 10,000 - 200 + 1 - 4 \\
&= 10,000 - 200 - 3 \\
&= 9,800 - 3 \\
&= 9,797 \\
&= 97 \cdot 101
\end{aligned}$$

Since both 97 and 101 are prime, $(99^2 - 4)^3 = 97^3 \cdot 101^3$.

Now, it is merely tedious to check that, by the Sylow theorems, $n_{97} | 101^3$ and $n_{97} \equiv 1 \mod 97$ implies that $n_{97} = 1$. Since the Sylow-97 subgroups P_{97} is a p group, it has non-trivial center by the class equation and so we obtain a subnormal series for P_{97}.

Namely,

$$1 \leq Z(P_{97}) \leq P_{97}$$

since $Z(P_{97}) = P_{97}$ so P_{97} is abelian, or $|Z(P_{97})| = 97, 97^2$ in which case $P_{97}/Z(P_{97})$ is abelian.

In any case, P_{97} is solvable.

Finally, since G/P_{97} is also a p-group of order 101^3, it will be solvable for the same reason.

Thus, G contains a normal solvable subgroup such that G/N is solvable and so G is solvable. ✌

Problem 2. For any finite group G and positive integer m, let $n_G(m)$ be the number of elements g of G that satisfy $g^m = e_G$. If A and B are finite abelian groups so that $n_A(m) = n_B(m)$ for all m, show that as groups $A \cong B$.

Solution. By the fundamental theorem of Abelian groups, we can write

$$A \cong (\mathbb{Z}_{p_1^{\alpha_1}})^{n_1} \oplus \cdots \oplus (\mathbb{Z}_{p_k^{\alpha_k}})^{n_k}$$
$$B \cong (\mathbb{Z}_{z_1^{\beta_1}})^{m_1} \oplus \cdots \oplus (\mathbb{Z}_{q_l^{\beta_l}})^{m_l}$$

with p_i, q_j primes, α_i, β_i distinct and n_i, m_j not zero. We note that $N_A(m), N_B(m) \geq 1$ for all m since e_A and e_B will always be counted.

Now, $N_A(p_i) > 1$ since each copy of $\mathbb{Z}_{p_i^{\alpha_i}}$ contains an element of order p_i by Lagrange's theorem.

However, $N_A(p_i) = N_B(p_i)$ and so then B contains a non-trivial element with order dividing p_i. Namely, B contains an element of order p_i.

Since p_i is prime and the q_i are primes, it must be that $p_i = q_j$ for some j.

Since this holds for all p_i and q_j, we can conclude that $k = l$ and $p_i = q_i$.

Now, $N_A(p_i^{\alpha_i}) = n_i(p_i^{\alpha_i} - 1) + 1$ since, if $g \in A$ satisfies that $g^{p_i^{\alpha_i}} = e_A$, then $g \in \mathbb{Z}_{p_i^{\alpha_i}}$. Since there are $p_i^{\alpha_i} - 1$ non-identity elements in each copy, and n_i copies plus 1 identity element, we conclude the above value.

In fact, $N_A(p_i^n) = n_i(p_i^{\alpha_i} - 1) + 1$ for all $n \geq \alpha_i$.

Therefore, $\beta_i = \alpha_i$ for all i. Else, if $N_B(p_i^{\beta_i})$ would be larger or smaller than $N_A(p_i^{\alpha_i})$.

Finally,

However, then

$$N_A(p_i^{\alpha_i}) = n_i(p_i^{\alpha_i} - 1) + 1 = m_i(p_i^{\alpha_i} - 1) + 1 = N_B(p_i^{\alpha_i})$$

and so $m_i = n_i$ for all i.

Therefore, $A \cong B$. ✌

Problem 3. If $g(x) = x^5 + 2 \in \mathbb{Q}[x]$, for $\mathbb{Q}$ the field of rational numbers, compute the Galois group of a splitting field L over $\mathbb{Q}$ of $g(x)$. How many subfields of L containing $\mathbb{Q}$ are Galois over $\mathbb{Q}$?

Solution. First, if $g(z) = 0$ then $z^5 = -2$. Letting $z = Re^{i\theta}$ we get that $R = \sqrt[6]{2}$ and $5\theta = (2k+1)\pi$ so, letting $z = e^{i\frac{\pi}{5}}$, we have that the roots of g are $Rz, -Rz^2, Rz^3, -Rz^4, Rz^5$.

Since $Rz^5 = -2 = -R\zeta^5$ where ζ is a primitive 5^{th}-root of unity, we can let $z = -\zeta$.

Thus, the splitting field for g is $L = \mathbb{Q}(R, \zeta)$.

Now, it is clear that $R\zeta$ has minimal polynomial g and so

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(R\zeta)][\mathbb{Q}(R\zeta) : \mathbb{Q}] = [L : \mathbb{Q}(R\zeta)]5$$

and similarly, ζ has minimal polynomial $x4 + x^3 + x^2 + x + 1$ and so

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\zeta)][\mathbb{Q}(\zeta) : \mathbb{Q}] = 4[\mathbb{Q}(\zeta) : \mathbb{Q}]$$

Thus, $20|[\mathbb{Q}(\zeta) : \mathbb{Q}]$ and since $[\mathbb{Q}(\zeta) : \mathbb{Q}] \geq 20$ we have that $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 20$.

Now, g is separable, the extension is Galois and so $|\mathrm{Gal}(g)| = [L : \mathbb{Q}] = 20$.

Now, we must work to identify $G = \mathrm{Gal}(g)$.

First, let

$$\begin{aligned} \sigma : L &\to L \\ R &\mapsto R\zeta \\ \zeta &\mapsto \zeta \end{aligned} \qquad\qquad \begin{aligned} \tau : L &\to L \\ R &\mapsto R \\ \zeta &\mapsto \zeta^3 \end{aligned}$$

Then both of these are automorphisms of L and furthermore, they do not commute since

$$\begin{aligned} \sigma(\tau(R)) &= \sigma(R) = R\zeta \\ \tau(\sigma(R)) &= \tau(R\zeta) = R\zeta^3 \end{aligned}$$

we have that G is not abelian.

Now,

$$\tau^4(\zeta) = \tau^3(\zeta^3) = \tau^2(\zeta^4) = \tau(\zeta^2) = \zeta$$

we have that τ is an element of order 4 and so G contains $\langle\tau\rangle \cong \mathbb{Z}_4$ as a subgroup.

Now, by the Sylow Theorems, $n_5 \equiv 1 \mod 5$ and $n_5|4$ so $n_5 = 1$. Namely, G has one Sylow 5-subgroup and it is normal.

Therefore,

$$0 \longrightarrow P_5 \longrightarrow G \longrightarrow P_4 \longrightarrow 0$$

is split because $P_5 \cap P_4 = \{e\}$ and so $|P_5P_4| = \frac{|P_5||P_4|}{|P_5 \cap P_4|} = \frac{5 \cdot 4}{1} = 20 = |G|$ and so

$$G \cong P_5 \rtimes P_4 \cong \mathbb{Z}_5 \rtimes \mathbb{Z}_4.$$

Finally, by the Galois Correspondence Theorem, to count the number of Galois extensions, we need to determine number of normal subgroups of G.

This requires exactly determining G up to isomorphism.

Let $\varphi : \mathbb{Z}_4 \to \mathrm{Aut}(\mathbb{Z}_5) \cong \mathbb{Z}_4$. We have already seen that $\langle \tau \rangle \cong P_4 \cong \mathbb{Z}_4$ and it is easy to show that $\langle \sigma \rangle = P_5 \cong \mathbb{Z}_5$

Then because G can be characterized as a semi-direct product, $\tau\sigma\tau^{-1} = \varphi(\tau)$.

Therefore, since

$$\tau(\sigma(\tau^{-1}(R))) = \tau(\sigma(R)) = \tau(R\zeta) = R\zeta^3 = \sigma^3(R).$$

Thus,

$$G \cong \langle \sigma, \tau \,|\, \sigma^5 = \tau^4 = 1, \tau\sigma\tau^{-1} = \sigma^3 \rangle.$$

Now, we must count normal subgroups of G.

The trivial subgroup as well as G itself are both normal subgroups and so L and $\mathbb{Q}$ are both Galois extensions of $\mathbb{Q}$.

We already have that P_5 is a normal subgroup and P_4 is not, so that adds one more. Note that P_4 is not normal since the above computation for G gave that

$$\sigma^{-1}\tau\sigma = \sigma^2\tau \notin P_4.$$

Namely,

$$\sigma(\tau(\sigma^{-1}(R))) = \sigma(\tau(R\zeta^4)) = \sigma(R\zeta^2) = R\zeta^3 \neq \tau^i$$

for any i.

Finally, if G has a subgroup of order 10 it will be normal since it will have index 2 which is the smallest prime dividing $|G|$. *(To see a proof of this see **Spring 2010, Problem 2, Claim 1**)*.

Now, if H is a subgroup of G of order 10, then it necessarily contains a copy of P_5 and since P_5 is the unique subgroup of G of order 5, $\sigma \in H$.

Now, it is not difficult to check that this forces $H = \langle \sigma, \tau^2 \rangle$ since if H must contain some power of τ^i with $i \neq 1$ (else $H = G$).

Thus, H is the unique normal subgroup of G of order 10.

Now, G is not a direct product since it is non-abelian and is defined as the semi-direct product of two abelian groups. Therefore, if G has a normal subgroup K of order 2 it must be contained in H, else $|HK| = \frac{|H||K|}{|H \cap K|} = \frac{10 \cdot 2}{1} = |G|$ and so $HK \cong H \times K \cong G$.

Now, if K is normal in G, then it must be normal in H and since $K \cong Q_2$ the Sylow 2-subgroup of H, it suffices to check if $n_2 = 1$ with $n_2 =$ the number of Sylow 2-subgroups of H.

However, $n_2 \neq 1$ since $\langle \tau^2 \rangle$ and $\langle \sigma^2\tau^2 \rangle$ both represent distinct Sylow 2-subgroups of H. This is because

$$(\sigma^2\tau^2)^2 = \sigma^2\tau^2\sigma^2\tau^2 = \sigma^2\tau\sigma\tau^3 = \sigma^2\sigma^3\tau^4 = 1.$$

Thus, $n_2 \neq 1$ and so G has no normal subgroups of degree 2.

Finally, the total number of Galois extensions of $\mathbb{Q}$ contained in L is $2+1+1=4$ which are associated to the trivial subgroup, G itself, P_5 which is G's Sylow 5-subgroup, and H the normal subgroup in G of order 10. ✌

Problem 4. Let P be a minimal prime ideal in the commutative ring R with 1; that is, if Q is a prime ideal in R and if $Q \subset P$, then $Q = P$. Show that each $x \in P$ is a zero divisor in R.

Solution. Let $S = R \backslash P$ as a set. Since P is a prime ideal, if $a, b \in R \backslash P$ then $ab \in R \backslash P$ (else if $ab \in P$ then $a \in P$ or $b \in P$ which is a contradiction).

Thus, S is closed under multiplication and since $0 \notin S$ (because $0 \in P$), $R' = S^{-1}R$ is a well defined ring.

Now, we claim that $PR' = \left\{ \frac{p}{s} \,|\, p \in P, s \in S \right\}$ is the unique maximal ideal of R'.

> **Claim 1.** PR' is the unique maximal ideal of R'.
>
> *Proof.* Let Q be an ideal of R'. If there exists some $\frac{q}{s} \in Q$ such that $\frac{q}{s} \notin PR'$, then $q \notin P$. However, then $q \in S$ and so $\frac{q}{q} = 1 \in Q$ and namely, $Q = R'$.
>
> Therefore, all proper ideals of R' are contained in PR'. ✌

> **Claim 2.** PR' is the unique prime ideal of R'.
>
> *Proof.* Now, assume that there is a Q prime ideal of R'. By the previous claim, $Q \subset P'R$. Thus, if $q \in Q$ then $\frac{p}{s} \in PR'$ so we have that $\frac{p}{s} = q \in Q$ for some q.
>
> Thus, $p = qs \in QS$ and so $qs \in P$. Therefore, $q \in P$ or $s \in P$.
>
> If $s \in P$ then $\frac{s}{s} = 1 \in PR'$ which is a contradiction since $P \neq R$. Thus, $q \in P$ and so namely, $QS \in P$. Since Q was assumed to be prime, QS will also be a prime ideal of R and so $P = QS$. Therefore, $Q = PR'$. ✌

Finally, we use the fact that the nilradical of R', which is the intersection of all prime ideals of R', which is exactly the set of nilpotent elements of R', is PR' (the only prime ideal of R').

Therefore, every element of PR' is nilpotent, and

$$\left(\frac{p}{s}\right)^n = \frac{p^n}{s^n} = 0 \implies p^n = 0$$

because S is closed under multiplication and does not contain 0 so namely, $s^n \neq 0$ for all $s \in S$ and all n.

Therefore, every element of P is nilpotent. ✌

Problem 5. Let $R = \mathbb{C}[x_1, ..., x_n]$ with $n \geq 3$ and $\mathbb{C}$ the field of complex numbers. Consider the ideal I of R defined by

$$I = (x_1 \cdots x_{n-1} - x_n, x_1 \cdots x_{n-2}x_n - x_{n-1}, ..., x_2 \cdots x_n - x_1)$$

so the generators of I are obtained by subtracting each x_j from the product of the others. Show that ther are fixed positive integers s and t so that for each $0 \leq i \leq n$, $(x_i^s - x_i)^t \in I$. (Hint: Consider the product of the generators of I.)

Solution. We examine $V(I)$.

First, if $x_i = 0$ for any i, then $x_k = 0$ for all k. This is immediate since $x_i = x_1x_2 \cdots x_{i-1}x_{i+1} \cdots x_{n-1}x_n$ for all i.

Now, taking $x_i \neq 0$ for all i, we have that

$$\begin{aligned}
x_i &= x_1 \cdots x_{i-1}x_{i+1} \cdots x_n \\
x_{i+1} &= x_1 \cdots x_i x_{i+2} \cdots x_n \\
\frac{x_{i+1}}{x_1 \cdots x_{i-1}x_{i+2} \cdots x_n} &= x_i \\
&= x_1 \cdots x_{i-1}x_{i+1} \cdots x_n \\
1 &= x_1^2 \cdots x_{i-1}^2 x_{i+2}^2 \cdots x_n^2 \\
&= \frac{x_i^2}{x_{i+1}^2} \\
x_i^2 &= x_{i+1}^2 \qquad \text{for all } i.
\end{aligned}$$

Therefore, as long as $x_i \neq 0$ for all i,

$$1 = x_i^{2(n-1)}$$

so namely, the x_i are equal to $2n-2$-roots of unity.

Namely,

$$x_i = x_i^{2n-1}$$

for all i. That is to say that $x_i^{2n-1} - x_i \in \sqrt{I}$ for all i and so namely, for each i, there exists a t such that $(x_i^{2n-1} - x_i)^t \in I$. ✌

Problem 6. Let R be a right artinian algebra over an algebraically closed field F. Show that R is algebraic over F of bounded degree. That is, show there is a fixed positive integer m so that for any $r \in R$ there is a non $g_r(x) \in F[x]$ with $g_r(r) = 0$ and with $\deg g \leq m$.

Solution. First, we note that $J(R/J(R)) = 0$ trivially.

Now, there is a correspondence between maximal ideals of $R/J(R)$ and max ideals of R containing $J(R)$. However, $J(R) \subset M$ for all M maximal ideals of R by definition and so there is a $1-1$ correspondence between max ideals of R and max ideals of $J(R)$.

Now, we claim that $R/J(R)$ has only finitely many maximal ideals.

Let

$$M_1 \supset M_1 M_2 \supset \cdots$$

be a descending chain of maximal ideals of $R/J(R)$. Because R is artinian, $R/J(R)$ is also artinian since quotients of artinian rings are artinian and so the chain terminates.

However, if the chain terminates at $M_1 \cdots M_n$, then these must be the only maximal ideals of $R/J(R)$.

> **Claim 3.** $M_1, ..., M_n$ are the only ideals of $R/J(R)$.
>
> *Proof.* Assume not, then if $x \in M_1 \cdots M_n$ and there is some maximal ideal of $R/J(R)$ such that $x \notin M$, we have that $MM_1 \cdots M_n \subsetneq M_1 \cdots M_n$ and therefore extends the chain which is a contradiction. ✌

Now, let

$$\varphi : R/J(R) \to \bigoplus_{i=1}^{n} \frac{R/J(R)}{M_i}$$
$$r \mapsto (r + M_1, ..., r + M_n)$$

Then φ is injective since clearly

$$\ker \varphi \subset \bigcap M_i = J(R/J(R)) = 0.$$

Furthermore, φ is clealry surjective so $R/J(R)$ is semi-simple since $(R/J(R))/M_i$ is a field for all i.

Therefore, by Artin-Wedderburn,

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

for some integers n_i and some division rings over F, D_i.

Namely, $R/J(R)$ is finite dimensional over F.

Now, because the center of D_i, $Z(D_i)$ is a field, by Schur's Lemma, $\psi : F \to Z(D_i)$ is either trivial or an isomoprhism.

However, F being commutative (by definition of field) and $R/J(R)$ being an algebra over F, we have that

$$F \in Z(R/(J(R))) \cong Z(M_{n_1}(D_1)) \oplus \cdots \oplus Z(M_{n_k}(D_k)0 \cong Z(D_1) \oplus Z(D_n)$$

and so namely, we can define a projection map to send $F \to Z(D_i)$ for all i. This map must be non-trivial for all i since $F \in Z(R/(J(R)))$ and so $F \cong Z(D_i)$ for all i.

Now, let $\alpha \in D_i$. Since $[F(\alpha) : F] < \infty$ (because $[D_i : F] < \infty$ by semi-simpleness of $R/J(R)$), we have that α is algebraic over F and thus satisfies a monic irreducible polynomial with coefficients in F. However, F is algebraically closed and so the only monic irreducible polynomials over F are linear. Namely, $\alpha \in F$.

Thus, $D_i = F$ for all i.

Now, $R/J(R)$ is a finite dimensional F-algebra and so $R/J(R)$ is algebraic over F. That is, $a + J(R)$ is algebaric over F for all $a \in R$.

Finally, $J(R)$ is algebraic over F because R is artinian and so $J(R)$ is nilpotent. Namely, x satisfies $x^n = 0$ for all $x \in J(R)$.

Since the sum of two algebraic elements is algebraic, this implies that $t = a + x$ and x is algebraic so $t - x = a$ is algebraic for all $a \in R$, and for all $x \in J(R)$. ✌