Kayla Orlinsky

Algebra Exam Fall 2011

Problem 1. Let I and J be ideals of $R = \mathbb{C}[x_1, x_2, ..., x_n]$ that define the same variety of $\mathbb{C}^n$. Show that for any $x \in (I+J)/I$ there is $m = m(x) > 0$ with $x^m = 0_{R/I}$. Show that there is an integer $M > 0$ so that for any $y_1, y_2, ..., y_M \in (I+J)/I$, $y_1 y_2 \cdots y_m = 0_{R/I}$.

Solution. To do this, we simply note the following claim.

> **Claim 1.** for I, J ideals of $k[x_1, ..., x_n]$, $V(I+J) = V(I) \cap V(J)$
>
> *Proof.* $\boxed{\supset}$ Let $\alpha \in V(I) \cap V(J)$. Then $f(\alpha) = 0$ for all $f \in I$ and $g(\alpha) = 0$ for all $g \in J$.
>
> However,
> $$I + J = \{\sum_{i=1}^{k} f_i g_i \mid f_i \in I, g_i \in J\}.$$
> Therefore, since f_i vanish and g_i vanish at α for all i, we get that $any h \in I + J$ will also vanish at α.
>
> Namely, $V(I+J) \supset V(I) \cap V(J)$.
>
> $\boxed{\subset}$ Since $I \subset I + J$ and $J \subset I + J$, $V(I+J) \subset V(I)$ and $V(I+J) \subset V(J)$. Therefore, $V(I+J) \subset V(I) \cap V(J)$. ✌

Now, by the **Claim 1**,

$$V(I+J) = V(I) \cap V(J) = V(I) \cap V(I) = V(I) \qquad V(I) = V(J) \text{ by assumption.}$$

Therefore, if $f(x) \in I + J$, then for all $\alpha \in V(I)$, $\alpha \in V(I+J)$ and so $f(\alpha) = 0$.

Thus, by Nullstellenzatz Part II, there exists an $m > 0$ such that $f^m \in I$.

Namely, if $\overline{f} \in (I+J)/I$, there exists m such that $\overline{f} = 0 \in R/I$.

Finally, since R is Noetherian by the Hilbert Basis Theorem, all ideals of R are finitely generated.

Therefore, if $J = (f_1(x), ..., f_n(x))$ we can let m_i, $i = 1, ..., n$ be the values found earlier such that $f_i^{m_i}(x) \in I$ for all i. Let $m = \max\{m_i\}$.

We would like to show that $[(I+J)/I]^{nm} = 0$. Note that

$$[(I+J)/I]^{nm} \cong [J/(I \cap J)]^{nm} \cong J^{nm}/(I \cap J)$$

by the second isomorphism theorem.

Now, we can let

$$J = Rf_1(x) \oplus \cdots \oplus Rf_n(x).$$

Then

$$J^{nm} = \bigoplus_{r_1+\cdots+r_n=nm} Rf_1^{r_1}(x)\cdots f_n^{r_n}(x).$$

Since $r_1+\cdots+r_n = nm$, there must exist some $r_i \geq m$. Otherwise, $r_1+\cdots+r_n < nm$. However, then $f_i^{r_i}(x) \in I$ by the above and so then $J^{nm} \subset I \cap J$ and so namely,

$$J^{nm}/(I\cap J) \cong [(I+J)/I]^{nm} = 0 \in R/I.$$

Therefore, $M = nm$ is such that any product of M things in $(I+J)/I$ will be trivial. ✌

Problem 2. . If $K \subset L$ are finite fields with $|K| = p^n$ and $[L : K] = m$ then show that for each $1 \le t < nm$, any $a \in L - K$ has a p^t-th root in L. When $m = 3$, show that every $b \in K$ has a cube root in L.

Solution. Since $|L| = p^{nm}$ L is the splitting field of $x^{p^{nm}} - x$.

Therefore, for all $a \in L$ and for all $1 \le t < nm$

$$a = a^{p^m} = a^{p^{nm-t}p^t} = \left(a^{p^{nm-t}}\right)^{p^t}.$$

Now, let $m = 3$, and let $b \in K$.

Then we can let

$$\begin{aligned} \varphi : L^\times &\to L^\times \\ a &\mapsto a^3 \end{aligned}$$

Since $L^\times \cong \langle a \rangle$ is a cyclic group of order $p^{3n} - 1$, we have two cases. First, if 3 is coprime to $p^{3n} - 1$, then φ is a group isomorphism. Namely, every element of L (and thus K) has a cube root in L.

If 3 is not coprime to $p^{3n} - 1$, then $3|(p^{3n} - 1)$ so $p^{3n} = 3t + 1$ some t.

Now, we want to show that $K^\times \subset \varphi(L^\times)$ since this will show that every $b \in K$ can be written as some $(a^x)^3$ for $a^x \in L$.

Now, if $a^x \in \ker\varphi$, then $(a^x)^3 = a^{3x} = 1$. However, then $\frac{p^{3n}-1}{3}$ divides x since the order of a is $p^{3n} - 1$. The converse is clearly also true. Thus, $x = 0, \frac{p^{3n}-1}{3}, 2\frac{p^{3n}-1}{3}$ and these are the only possibilities. Namely,

$$|\varphi(L^\times)| = \frac{|L^\times|}{|\ker\varphi|} = \frac{p^{3n} - 1}{3}.$$

Now, since $\varphi(L^\times) = \langle a^x \rangle$ is also cyclic, letting $K^\times = \langle a^y \rangle$ for some y, we have that $K^\times \subset \varphi(L^\times)$ if $x|y$.

Claim 2. x divides y if and only if $(p^n - 1)$ divides $\frac{p^{3n}-1}{3}$.

Proof. $\boxed{\Longrightarrow}$ If $x|y$ then $K^\times \subset \varphi(L^\times)$ and so $|K^\times| = p^n - 1$ must divide $|\varphi(L^\times)| = \frac{p^{3n}-1}{3}$.

$\boxed{\Longleftarrow}$ Assume $(p^n - 1)$ divides $\frac{p^{3n}-1}{3}$. Then the order of a^y divides the order of a^x.

Namely,

$$(a^x)^{\frac{p^{3n}-1}{3}} = (a^x)^{(p^n-1)t} = (a^{xt})^{p^n-1} = 1 = (a^y)^{p^n-1}$$

for some t.

And so the order of a^{xt} is $p^n - 1$ as well. Thus, $\langle a^{xt} \rangle = \langle a^y \rangle$ and so $x|y$. ✌

From the claim, we need only show that $(p^n - 1)$ divides $\frac{p^{3n}-1}{3}$.

However, $\frac{p^{3n}-1}{3} = \frac{(p^n-1)(p^{2n}+p^n+1)}{3}$.

If $3|(p^{2n} + p^n + 1)$ then we are done, so assume not.

Then $3|(p^n - 1)$. Namely, $p^n \equiv 1 \mod 3$. So $p^{2n} + p^n + 1 \equiv 1 + 1 + 1 \equiv 0 \mod 3$ and so again, $3|(p^{2n} + p^n + 1)$.

Therefore, $p^n - 1$ divides $(p^n - 1)\frac{p^{2n}+p^n+1}{3}$ and so $K^\times \subset \varphi(L^\times)$ is a subgroup.

Finally, this gives that for every $b \in K$, b has a cube root in L. ✌

Problem 3. Let F be an algebraically closed field and A an F-algebra with $\dim_F A = n$. If every element of A is either nilpotent or invertible, show that the set of nilpotent elements of A is an ideal M of A, that M is the unique maximal ideal of A, and that $\dim_F M = n - 1$.

Solution. Let M be the set of nilpotent elements of A. Namely, M is the nilradical of A. M is always an ideal since A is commutative (being an algebra) and so if $x, y \in M$ with $x^s = 0$ and $y^t = 0$, then $(x-y)^{st} = 0$ and so $x - y \in M$. Similarly, if $a \in A$ then $(ax)^s = a^s x^s = 0$ so $ax \in M$.

Thus, M is an ideal.

Now, let $M \subsetneq M' \subset A$ with M' another ideal of A.

Then let $x \in M'$ and $x \notin M$. Since x is not nilpotent, it is invertible. Therefore, $x^{-1}x = 1 \in M'$ and so $M' = A$.

Thus, M is maximal.

Using this same argument, we get that M must be unique, since any other element not in M is invertible and so cannot be contained in any proper ideal.

Finally, since A/M is a field, it is a field extension of F. However, since F is algebraically closed, $A/M \cong F$.

Therefore,

$$1 = \dim_F(A/M) = \dim_F A - \dim_F M = n - \dim_F M \implies \dim_F M = n - 1.$$

✌

Problem 4. Let M be a finitely generated $F[x]$ module, for F a field.

(a) Show that if $f(x)m = 0$ for $f(x) \neq 0$ forces $m = 0$, then M is a projective $F[x]$ module.

(b) If H is an $F[x]$ submodule of M show that $M = H \oplus K$ for a submodule K of M if and only if: $f(x)m \in H$ for $f(x) \neq 0$ implies $m \in H$.

Solution.

(a) Since M is finitely generated over $F[x]$ which is a PID, we may apply the structure theorem. Note also that because $F[x]$ is a PID, projective is equivalent to free.

Thus, by the structure theorem,

$$M \cong P \oplus T(M)$$

with P the free part of M and $T(M)$ the torsion part.

Now, let $m \in T(m)$. Then there exists $f(x) \in F[x]$ with $f(x) \neq 0$ such that $f(x)m = 0$. However, by assumption, this implies that $m = 0$.

Thus, $T(M) = 0$ and so $M \cong P$ for some free module P. Therefore, M is free and so it is projective.

(b) $\boxed{\Longrightarrow}$ Assume H is an $F[x]$ submodule of M.

Further, assume that $M = H \oplus K$ for a submodule K of M.

Because M is free, H is free, and so $H \cap K = (0)$ because H is projective.

Now, let $f(x)m \in H$ for $f(x) \neq 0$. If $m \notin H$, then $m \in K$ because $M = H \oplus K$ and $H \cap K = (0)$.

However, then $f(x)m \in K$ because K is a submodule, which is a contradiction.

Thus, $m \in H$.

$\boxed{\Longleftarrow}$ Assume if $f(x)m \in H$ and $f(x) \neq 0$, then $m \in H$.

Then, by (a), H is projective, and so letting $\varphi : M \to H$ be any surjective homomorphism, (which exists since both M and H are free and have bases over $F[x]$) we get a short exact sequence of the form

$$0 \longrightarrow K \longrightarrow M \longrightarrow H \longrightarrow 0$$

where $K = \ker \varphi$.

Since H is projective, the sequence is split and $M \cong H \oplus K$ so we are done.

✌

Problem 5. Up to isomorphism, describe the possible structures of any group of order $987 = 3 \cdot 7 \cdot 47$.

Solution. $\boxed{\text{Abelian}}$ There is an abelian group of order 987 isomorphic to

$$G \cong \mathbb{Z}_3 \times \mathbb{Z}_7 \times \mathbb{Z}_{47}.$$

Now, for G non-abelian, using the Sylow theorems it is immediate that $n_{47} = 1$ since $n_{47}|21$ and $n_{47} \equiv 1 \mod 47$ so $n_{47} = 1$.

Thus, G has a normal Sylow 47-subgroup. Let P_{47} be the normal Sylow 47-subgroup, and P_3, P_7 be Sylow 3-subgroups and Sylow 7-subgroups.

> **Claim 3.** If N is normal in G and P is a normal Sylow p-subgroup of N, then P is normal in G.
>
> *Proof.* Let N be normal in G and P be a normal Sylow p-subgroup of N.
>
> Let $g \in G$. Then $gNg^{-1} = N$, therefore, since P is a subgroup of N, $gPg^{-1} \subset N$.
>
> Therefore, if $p \in P$, $gpg^{-1} = n \in N$. However, conjugation is an automorphism and preserves order, so $n \in N$ has order dividing $|P|$. Thus, n lies in some Sylow p-subgroup of N. However, since P is normal in N, P is the only Sylow p-subgroup of N and so $n \in P$.
>
> Thus, $G = N_G(P)$. ✌

Therefore, since P_{47} is normal, P_7P_{47} is a subgroup of G and since it has index 3 which is the smallest prime dividing the order of G, it is normal by **Spring 2010: Problem 2 Claim 1**.

Clearly P_7 is normal in P_7P_{47} since $n_7|47$ and $n_7 \equiv 1 \mod 7$ so $n_7 = 1$ so by **Claim 3**, P_7 is normal in G.

$\boxed{P_{47} \rtimes P_3 \times P_7}$. Let $\varphi : P_3P_7 \to \text{Aut}(P_{47})$. Since $P_{47} \cong \mathbb{Z}_{47}$,

$$\varphi : \mathbb{Z}_{21} \to \mathbb{Z}_{47}^{\times} \cong \mathbb{Z}_{46}.$$

Since $\mathbb{Z}_{46}$ has no elements of order 3 or order 7, φ can only be the trivial homomorphism and this gives no new group structures aside from the abelian one.

Now, since P_{47} is normal, $P_{47}P_3$ and $P_{47}P_7$ are subgroups of G.

$\boxed{P_3 \rtimes P_7 \times P_{47}}$ if $P_3 \trianglelefteq G$, then by similar arguments as before, $G \cong P_3 \rtimes P_7 \times P_{47}$.

Let

$$\varphi : \mathbb{Z}_{7 \cdot 47} \to \text{Aut}(P_3) \cong \mathbb{Z}_2.$$

Since there are no order 2 elements in $\mathbb{Z}_{7\cdot 47}$ this gives nothing interesting.

$\boxed{P_7 \times P_{47} \rtimes P_3}$ Since 3 is the smallest prime dividing $|G|$, and $[G : P_7P_{47}] = 3$, and $P_7P_{47} \cong P_7 \times P_{47}$ is subgroup of G, and it is normal by **Spring 2010, Problem 2, Claim 1**.

Let

$$\varphi : P_3 \to \mathrm{Aut}(P_7 \times P_{47}) \cong \mathrm{Aut}(P_7) \times \mathrm{Aut}(P_{47}) \cong \mathbb{Z}_6 \times \mathbb{Z}_{46}.$$

There are exactly two elements of order 3 in $\mathbb{Z}_6 \times \mathbb{Z}_{46}$, namely $(2, 0)$ and $(4, 0)$.

Thus, we have two non-trivial homomorphisms, $\varphi_1(1) = (2, 0)$ and $\varphi_2(1) = (4, 0)$.

Let $P_3 \cong \langle a\rangle$ and $P_7 \times P_{47} \cong \langle b\rangle \times \langle c\rangle$.

Then $(2, 0)$ and $(4, 0)$ correspond to the maps ψ_1 and ψ_2 respectively, with

$$\begin{aligned} \psi_1 : \langle b\rangle \times \langle c\rangle &\to \langle b\rangle \times \langle c\rangle \\ (b, c) &\mapsto (b^2, c) \end{aligned} \qquad \begin{aligned} \psi_2 : \langle b\rangle \times \langle c\rangle &\to \langle b\rangle \times \langle c\rangle \\ (b, c) &\mapsto (b^4, c) \end{aligned}$$

It is crucial to note that $\psi_2 = \psi_1^2$.

Thus, if

$$\begin{aligned} \gamma : P_3 &\to P_3 \\ a &\mapsto a^2 \end{aligned}$$

then γ is an automorphism of P_3 since a^2 also a generator of P_3 and since $\varphi_2 = \varphi_1 \circ \gamma$, we get that φ_2 and φ_1 define isomorphic semi-direct products.

Thus, the multiplication for φ_1 is $aba^{-1} = \varphi_1(a)(b) = \psi_1(b) = b^2$ and $aca^{-1} = \varphi_1(a)(c) = \psi_1(c) = c$.

And so we get one group,

$$G \cong \mathbb{Z}_7 \times \mathbb{Z}_{47} \rtimes_{\varphi_1} \mathbb{Z}_3 = \langle a, b, c \,|\, a^3 = b^7 = c^{47} = 1, ac = ca, bc = cb, ab = b^2a\rangle$$

$\boxed{P_3 \times P_{47} \rtimes P_7}$ If P_3 is normal, then $P_3 \times P_{47}$ is a normal subgroup of G and so we can examine

$$\varphi : P_7 \to \mathrm{Aut}(P_3 \times P_{47}) \cong \mathbb{Z}_2 \times \mathbb{Z}_{46}.$$

However, again, no non-trivial homomorphism exists.

$\boxed{P_7 \rtimes P_3 \times P_{47}}$ If P_7 is normal, then we can look at

$$\varphi : \mathbb{Z}_3 \times \mathbb{Z}_{47} \to \mathrm{Aut}(P_7) \cong \mathbb{Z}_6$$

However, this will give two non-trivial homomorphisms, $\varphi_1(1) = (2)$ and $\varphi_2(1) = 4$.

Since these automorphisms are given by $\psi_1(b) = b^2$ and $\psi_2(b) = b^4$, we quickly see that both of these yield the same multiplicative structure as before.

Namely, for φ_1 we get $aba^{-1} = b^2$ and $cbc^{-1} = b$ and for φ_2 we get $aba^{-1} = b^4$ and $cbc^{-1} = b$ and $ac = ca$. These were already described in an earlier case.

$\boxed{P_3 \times P_7 \rtimes P_{47}}$ If $P_3 \times P_7$ is normal, then we can examine

$$\varphi : P_{47} \to \mathrm{Aut}(P_3 \times P_7) \cong \mathbb{Z}_2 \times \mathbb{Z}_6.$$

Clear this forces φ to be trivial.

Therefore, there are exactly 2 possible groups up to isomorphism.

$$\boxed{\begin{gathered} \mathbb{Z}_3 \times \mathbb{Z}_7 \times \mathbb{Z}_{47} \\ \langle a, b, c \,|\, a^3 = b^7 = c^{47} = 1, ac = ca, bc = cb, ab = b^2a \rangle \end{gathered}}$$

✌

Problem 6. Let $R = \mathbb{Z}[x_1, x_2, ..., x_n, ...]$ and let $\{f_i(X) \,|\, i \geq 1\} \subseteq R$ satisfy

$$f_1(X)R \subseteq f_2(X)R \subseteq \cdots \subseteq f_t(X)R \subseteq \cdots .$$

Show that $f_s(X)R = f_m(X)R$ for some m and all $s \geq m$.

Solution. Since each f_i is a polynomial, we may take each f_i to be comprised of a finite number of variables.

Namely, $f_1 \subset \mathbb{Z}[x_{k_1}, ..., x_{k_{n_1}}]$ for some k_j.

Now, $(f_1(X)) \subset (f_2(X))$ and so there exists $g_2(X)$ such that $f_1(X) = f_2(X)g_2(X)$.

Now, since $\mathbb{Z}$ is a UFD, $\mathbb{Z}[x_{k_1}, ..., x_{k_{n_1}}]$ is also a UFD, and so f_1 can be uniquely factored into irreducibles (which are primes in a UFD), $f_1 = p_1 \cdots p_t$.

Then, since

$$f_1(X) = p_1(X) \cdots p_t(X) = f_2(X)g_2(X)$$

we get that $f_2 g_2 \in \mathbb{Z}[x_{k_1}, ..., x_{k_{n_1}}]$ and so each p_j divides either f_2 or g_2

Namely, $f_2(X) \in \mathbb{Z}[x_{k_1}, ..., x_{k_{n_1}}]$.

Therefore, inductively, we get that $f_i(X) \in \mathbb{Z}[x_{k_1}, ..., x_{k_{n_1}}]$ for all i and so namely, if $R' = \mathbb{Z}[x_{k_1}, ..., x_{k_{n_1}}]$, then we can write

$$f_1(X)R' \supset f_2(X)R' \supset \cdots .$$

Since $\mathbb{Z}$ is Noetherian, by the Hilbert Basis Theorem, $R' = \mathbb{Z}[x_{k_1}, ..., x_{k_{n_1}}]$ is also Noetherian and so the chain must terminate at some finite m.

Since $(f_m(X)) = (f_n(X)) \subset R' \subset R$ for all $n \geq m$, we are done. ✌

Problem 7. Let U be the set of all n-th roots of unity in $\mathbb{C}$, for all $n \geq 3$, and set $F = \mathbb{Q}(U)$. For primes $p_1 < \cdots < p_k$ and nonzero $a_1, ..., a_k \in \mathbb{Q}$, set $M = F(a_1^{1/p_1}, ..., a_k^{1/p_k}) \subseteq \mathbb{C}$. Show that M is Galois over F with a cyclic Galois group. For any subfield $F \subseteq L \subseteq M$, show that there is a subset T of $\{a_j^{1/p_j}\}$ so that $L = F(T)$.

Solution. M is Galois over F if M is the splitting field of a separable polynomial over F.

Since a_i^{1/p_i} has minimal polynomial $f_i(x) = x^{p_i} - a_i$, which has roots $\xi_i^l a_i^{1/p_i}$ for ξ_i a p_i^{th} root of unity and $0 \leq l \leq p_i - 1$, f_i splits completely in M.

Therefore, M is the splitting field of $\prod_{i=1}^k f_i(x)$ which is a polynomial over F. Thus, M is Galois over F.

Note that $[M : F] \leq \prod_{i=1}^k p_i$. However,

$$[M : F] = [M : F(a_i^{1/p_i})][F(a_i^{1/p_i}) : F] = [M : F(a_i^{1/p_i})]p_i$$

and so $p_i | [M : F]$ for all $i = 1, ..., k$. Therefore, $[M : F] = p_1 \cdots p_k$.

Now, let $G = \text{Gal}(M/F)$. Using the same logic, we obtain that

$$K = F(a_1^{1/p_1}, ..., a_{i-1}^{1/p_{i-1}}, a_{i+1}^{1/p_{i+1}}, ..., a_k^{1/p_k}) \text{ is Galois over } F$$

and since $[M : K] = p_i$, G has a normal subgroup of order p_i. Namely, G has a normal Sylow p_i-subgroup for all i.

This is only possible if G is abelian and so

$$G \cong \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_k} \cong \mathbb{Z}_{p_1 \cdots p_k} \qquad \text{cyclic.}$$

Finally, let $F \subset L \subset M$.

Then L corresponds to some subgroup of G. However, the subgroups of G correspond exactly to products of the $\mathbb{Z}_{p_i}$. Thus, if L corresponds to $\mathbb{Z}_{p_{i_1}} \times \cdots \times \mathbb{Z}_{p_{i_l}}$ with $l \leq k$, then $L = F(a_{i_1}^{1/p_{i_1}}, ..., a_{i_l}^{1/p_{i_l}})$. ✌