Kayla Orlinsky

Algebra Exam Fall 2015

Problem 1. If M is a maximal ideal in $\mathbb{Q}[x_1, ..., x_n]$ show that there are only finitely many maximal ideals in $\mathbb{C}[x_1, ..., x_n]$ that contain M.

Solution. This question is actually a specific case of **Spring 2015: Problem 3**.

First, we note that by Nullstellensatz, since M is a proper ideal of $\mathbb{Q}[x_1, ..., x_n]$, $V(M) \neq \varnothing$ as a subset of $\mathbb{C}^n$. Namely, there exists $(a_1, ..., a_n) \in \mathbb{C}^n$ such that every polynomial in M is satisfied by $(a_1, ..., a_n)$.

Thus, by Nullstellensatz, for every $f \in M$ considered as a polynomial in $\mathbb{C}[x_1, ..., x_n]$, there exists r such that $f^r \in (x_1 - a_1, ..., x_n - a_n)$. However, by Nullstellensatz, $(x_1 - a_1, ..., x_n - a_n)$ is a maximal ideal of $\mathbb{C}[x_1, ..., x_n]$ and so it is prime. Thus, recursively, $f \in (x_1 - a_1, ..., x_n - a_n)$, for all $f \in M$.

Thus, $M \subset (x_1 - a_1, ..., x_n - a_n)$.

Therefore, M is contained in at least one maximal ideal of $\mathbb{C}[x_1, ..., x_n]$.

Now, for each maximal ideal $N \subset \mathbb{C}[x_1, ..., x_n]$ such that $M \subset N$, there is clearly an induced injection of fields

$$\mathbb{Q}[x_1, ..., x_n]/M \hookrightarrow \mathbb{C}[x_1, ..., x_n]/N$$

where $L = \mathbb{Q}[x_1, ..., x_n]$ is a field extension of $\mathbb{Q}$ and $\mathbb{C}[x_1, ..., x_n]/N \cong \mathbb{C}$ since $\mathbb{C}$ is algebraically closed and so the only field extension of it is itself.

Clearly, the correspondence is 1-to-1. Namely, for every distinct maximal ideal N containing M there corresponds one injection of fields from L into $\mathbb{C}$.

Now we prove two claims. First, that $L/\mathbb{Q}$ is finite, and second that there are only finitely many injections from a finite field extension of $\mathbb{Q}$ into its algebraic closure.

Both of these were proved in **Spring 2015: Problem 3 Claim 1, Claim 2.**

Both claims are proved by induction.

First, we argue that L is an algebraic extension of $\mathbb{Q}$ (and hence finitely generated), then we argue that any injection of L into $\mathbb{C}$ is uniquely determined by how it permutes the roots of the minimal polynomial of each generator of L, of which there are only finitely many options.

Finally, we obtain that there are only finitely many maximal ideals N of $\mathbb{C}[x_1, ..., x_n]$ containing M. ✌

Problem 2. Let R be a right Noetherian ring with 1. Prove that R has a *unique* maximal nilpotent ideal $P(R)$. Argue that $R[x]$ also has a unique maximal nilpotent ideal $P(R[x])$. Show that $P(R[x]) = P(R)[x]$.

Solution. Let $\mathcal{S}$ be the set of nilpotent right-ideals of R.

Since R is right-Noetherian, every set of ideals contains a unique maximal element. Thus, $\mathcal{S}$ contains a maximal nilpotent right ideal N of order n.

Let J be a second such maximal ideal of order j. Then $J + N = \{a + b \mid a \in J, b \in N\}$ will also be a nilpotent ideal since $(a + b)^{jn} = 0$.

Since $N \subset J + N$ and N is maximal, $J + N = N$, however $J \subset J + N$ as well and so $J + N = J$. Therefore, $N = J$. Thus, N is unique.

Now, let $P(R)$ be the two-sided ideal generated by N. We would like to show that $P(R)$ is nilpotent.

Let $x_1, ..., x_n, x_{n+1} \in N$, and $r_1, ..., r_n, r_{n+1} \in R$. It suffices to show that any product of k things of the form nr where $n \in N$ and $r \in R$ is 0 for some k.

Then

$$(x_1 r_1)(x_2 r_2) \cdots (x_n r_n)(x_{n+1} r_{n+1}) = x_1(r_1 x_2)(r_2 x_3) \cdots (r_n x_{n+1}) r_{n+1} = x_1 0 r_{n+1} = 0$$

since $r_i x_i \in N$ and N is nilpotent of order n.

Therefore, $P(R)$ is nilpotent of order at most $n + 1$. Since $P(R)$ is generated by the unique maximal nilpotent right-ideal of R, it is the unique maximal nilpotent 2-sided ideal of R.

By the Hilbert Basis theorem, $R[x]$ is also right-Noetherian, and so it too will contain a unique maximal 2-sided nilpotent ideal, $P(R[x])$

Let $f(x) = a_m x^m + \cdots + a_1 x + a_0 \in P(R[x])$. We induct on the degree of f.

If $f(x) = a_0$, then $f^n = a_0^n = 0$ so trivially $f(x) \in P(R)[x]$.

Assume $f \in P(R[x]) \implies f \in P(R)[x]$ for f having degree $k \le m - 1$.

Now, assume f has degree m.

Because $f^n = 0$, we have that $a_m^n = 0$, so $a_m x^m \in P(R)[x]$. Therefore, $f - a_m x^m \in P(R)[x]$ by the inductive hypothesis since $f - a_m x^m$ has degree strictly less than m and is a sum of nilpotent elements (which is also nilpotent).

Therefore, since $f - a_m x^m \in P(R)[x]$ and $a_m x^m \in P(R[x])$, we have that $f \in P(R)[x]$.

If $f(x) \in P(R)[x]$, then every coefficent of f is nilpotent of degree less than or equal to n, so $f^{n^2}(x) = 0$ since each coefficient will be raised to at least the n^{th} power. Therefore, $f \in P(R[x])$ since this is the unique largest nilpotent ideal of $R[x]$.

✌

Problem 3. Up to isomorphism, describe the possible structures of any group of order 182 as a direct sum of cyclic groups, dihedral groups, other semi-direct products, symmetric groups, or matrix groups. (Note: 91 is not prime!)

Solution. Let G be a group of order $182 = 2 \cdot 7 \cdot 13$. By Sylow, $n_7 \equiv 1 \mod 7$ and $n_7 | 2 \cdot 13$. Therefore, $n_7 = 1$ so G has a normal Sylow 7-subgroup.

Abelian By the fundamental theorem of abelian groups, $G \cong \mathbb{Z}_{182}$.

Let P_2, P_7, P_{13} be Sylow $2, 7, 13$-subgroups of G respectively.

Therefore, $P_7 P_{13}$ is a subgroup of G and it is normal in G since it has index 2 which is the smallest prime dividing the order of G. (see **Spring 2010: Problem 2 Claim 1**).

Now, in $P_7 P_{13}$, because $n_{13} | 7$ and $n_{13} \equiv 1 \mod 13$, $n_{13} = 1$ so $P_7 P_{13}$ has a normal Sylow 13-subgroup.

Therefore, because P_{13} is normal in $P_7 P_{13}$ which is normal in G, P_{13} is also normal in G so G has one normal Sylow 13-subgroup (see **Fall 2011: Problem 5 Claim 3**).

Thus, we need to check only three homomorphisms.

$\varphi : P_2 P_7 \to \text{Aut}(P_{13})$ Since P_7 is normal, $P_2 P_7$ is a subgroup of G. Let $\varphi : P_2 P_7 \to \text{Aut}(P_{13}) \cong \mathbb{Z}_{13}^{\times} \cong \mathbb{Z}_{12}$.

Let $P_2 \cong \langle a \rangle$, $P_7 \cong \langle b \rangle$, $P_{13} \cong \langle c \rangle$.

Then since there are no elements of order 7 in $\mathbb{Z}_{12}$, $\varphi(b) = \text{Id}$.

There is one possible elements of order 2 to send a, namely, $\varphi(a) = \alpha$ where $\alpha(c) = c^{12}$. This defines multiplication on G by $aca^{-1} = \varphi_1(a)(c) = c^{12} = c^{-1}$

$$G \cong \langle a, b, c \,|\, a^2 = b^7 = c^{13} = 1, ab = ba, bc = cb, ac = c^{-1}a \rangle$$

We note that

$$G \cong \mathbb{Z}_{13} \rtimes_{\varphi_1} \mathbb{Z}_2 \times \mathbb{Z}_7 \cong D_{26} \times \mathbb{Z}_7$$

where D_{26} is the dihedreal group of 26 elements.

$\varphi : P_2 P_{13} \to \text{Aut}(P_7)$ $\varphi : P_2 P_{13} \to \mathbb{Z}_6$. We have one choice: $\varphi_2(c) = \text{Id}$, and $\varphi_2(a) = \beta$ where $\beta(b) = b^5 = b^{-1}$, since this is the only element of $\text{Aut}(P_7)$ of order 2.

This gives

$$G \cong \langle a, b, c \,|\, a^2 = b^7 = c^{13} = 1, ac = ca, bc = cb, ab = b^{-1}a \rangle \cong D_{14} \times \mathbb{Z}_{13}.$$

$\varphi : P_2 \to \text{Aut}(P_7 P_{13})$ Let $\varphi : P_2 \to \text{Aut}(P_7 P_{13}) \cong \text{Aut}(P_{13}) \times \text{Aut}(P_7)$ since 7 and 13 are coprime and P_7 and P_{13} are cyclic.

Now, defining $\varphi(a) = (\alpha, \text{Id})$ or $\varphi(\text{Id}, \beta)$ will yield the same multiplication as we found previously.

Thus, the only new structure can be given by $\varphi(a) = (\alpha, \beta)$.

Therefore, we get one more possible structure for G.

$$G \cong \langle a, b, c \,|\, a^2 = b^7 = c^{13} = 1, ac = c^{-1}a, bc = cb, ab = b^{-1}a \rangle \cong D_{182}.$$

Finally, we have 4 possible group structures for G.

$$\mathbb{Z}_{182}$$

$$D_{14} \times \mathbb{Z}_{13}$$

$$D_{26} \times \mathbb{Z}_7$$

$$D_{182}$$

✌

Problem 4. Let $K = \mathbb{C}(y)$ for an indeterminate y and let $p_1 < p_2 < \cdots < p_n$ be primes (in $\mathbb{Z}$). Let $f(x) = (x^{p_1} - y) \cdots (x^{p_n} - y) \in K$ with splitting field L over K.

(a) Show each $x^{p_j} - y$ is irreducible over K

(b) Describe the structure of $\text{Gal}(L/K)$.

(c) How many intermediate fields are between K and L.

Solution. This problem is a more extensive version of **Fall 2013: Problem 7**

(a) We use generalized Eisenstein's criterion with $p = y$. Clearly (y) is a prime (in fact maximal) ideal since $\mathbb{C}(y)/(y) \cong \mathbb{C}$ which is a domain.

Now, $0 \in (y)$ and $y \in (y)$ and $1 \notin (y)$ which is the criterion on the coefficeints of $x^{p_j} - y$. Finally, $y \notin (y)^2$ and so $x^{p_j} - y$ is irreducible over K.

(b) Each irreducible $x^{p_j} - y$ factor of f has as its roots, the p_j roots of y multiplying the p_j^{th} roots of unity. Namely, f is separable and so L/K is indeed Galois.

Furthermore, each $\sigma \in G = \text{Gal}(L/K)$ 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 $x^{p_j} - y$, fixing the other roots of f.

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,

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

(c) Since G is abelian, any product of subgroups of G will also be a subgroup and so there are

$$\sum_{i=1}^{n-1} \binom{n}{i} = \sum_{i=0}^{n} \binom{n}{i} - 2 = 2^n - 2$$

possible subgroups.

✌

Problem 5. In any finite ring R with 1 show that some element in R is not a sum of nilpotent elements. Note that in all $M_n(\mathbb{Z}/n\mathbb{Z})$ the identity matrix is a sum of nilpotent elements. (Hint: What is the trace of a nilpotent element in a matrix ring over a field?)

Solution. Since R is finite, it is clearly artinian. Thus, by Artin Wedderburn, $R/J(R)$ is semi-simple and so isomorphic to $M_{n_1}(D_1) \oplus \cdots \oplus M_{n_k}(D_k)$ where D_i are division rings over R.

Since the only finite division rings are finite fields, we have that

$$R/J(R) \cong M_{n_1}(\mathbb{F}_{q_1}) \oplus \cdots \oplus M_{n_k}(\mathbb{F}_{q_k})$$

where $\mathbb{F}_{q_i}$ is the field of q_i elements.

Now, we note that the trace $\text{tr}(A) = 0$ if $A \in M_n(\mathbb{F}_q)$ is nilpotent.

Therefore, if A is a sum of nilpotent matrices $A = N_1 + \cdots + N_l$ then

$$\text{tr}(A) = \text{tr}(N_1 + \cdots + N_l) = \text{tr}(N_1) + \cdots + \text{tr}(N_l) = 0 + \cdots + 0 = 0.$$

Therefore, if $\text{tr}(A) \neq 0$ then A cannot be a sum of nilpotent elements.

Let

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

Then A is not nilpotent, and it is not a sum of nilpotents since $\text{tr}(A) = 1 \neq 0$ over any finite field.

Since $A + J(R)$ is not a sum of nilpotent elements of $R/J(R)$, A cannot be a sum of nilpotent elements of R. ✌

Problem 6. Let R be a commutative principal ideal domain.

(a) If I and J are ideals of R show that $R/I \otimes_R R/J \cong R/(I+J)$.

(b) If V and W are finitely generated R modules so that $V \otimes_R W = 0$, show that V and W are torsion modules whose annihilators in R are relatively prime.

Solution.

(a) Let I and J be ideals of R. Define

$$\begin{aligned} f : R/I \times R/J &\to R/(I+J) \\ (a+I, b+J) &\mapsto ab + I + J \end{aligned}$$

Then f is well defined since if $(a+I, b+J) = (a'+I, b'+J)$ then $a = a'+i$ for $i \in I$ and $b = b'+j$ for $j \in J$.

Thus,

$$\begin{aligned} f(a+I, b+J) &= ab + I + J \\ &= (a'+i)(b'+j) + I + J \\ &= a'b' + a'j + b'i + ij + I + J \\ &= a'b' + I + J \\ &= f(a'+I, b'+J) \end{aligned}$$

Furthermore,

$$f(ra+I, b+J) = rab + I + J = rf(a+I, b+J)$$

and

$$f(a+I, br+J) = abr + I + J = f(a+I, b+J)r$$

since R is commutative.

Finally,

$$f(a+a'+I, b+J) = (a+a')b + I + J = f(a+I, b+J) + f(a'+I, b+J)$$

and similarly for linearity on the right.

Thus, f is bilinear.

Thus, because R is commutative $R/(I+J)$ is an abelian group under multiplication. Thus, by the universal property of tensor product, f induces a map $\overline{f} : R/I \otimes_R R/J \to R/(I+J)$ defined by $\overline{f}((a+I) \otimes (b+J)) = ab + I + J$.

Let $r \in R/I \otimes_R R/J$ then

$$\begin{aligned} r &= \sum_{i=1}^{n} (a_i + I) \otimes (b_i + J) \\ &= \sum_{i=1}^{n} (a_i + I) \otimes b_i(1 + J) \\ &= \sum_{i=1}^{n} b_i(a_i + I) \otimes (1 + J) \\ &= \sum_{i=1}^{n} (b_i a_i + I) \otimes (1 + J) \\ &= \left(\sum_{i=1}^{n} b_i a_i + I \right) \otimes (1 + J) \end{aligned}$$

Thus, $r = (s + I) \otimes (1 + J)$ for some $s \in R$.

Now, $g : R/(I + J) \to R/I \otimes_R R/J$ defined by $g(a + I + J) = (a + I) \otimes 1$.

Then g is clearly well defined since if $a + I + J = b + I + J$ then there exists $i, j \in I, J$ respectively so $a + I + J = b + i + j + I + J$. Thus,

$$\begin{aligned} g(a + I + J) &= (a + I) \otimes (1 + J) \\ &= (b + i + j + I) \otimes (1 + J) \\ &= (b + I) \otimes (1 + J) + (j + I) \otimes (1 + J) \\ &= (b + I) \otimes (1 + J) + j(1 + I) \otimes (1 + J) \\ &= (b + I) \otimes (1 + J) + (1 + I) \otimes (j + J) \\ &= (b + I) \otimes (1 + J) + (1 + I) \otimes 0 \\ &= (b + I) \otimes (1 + J) \\ &= g(b + I + J) \end{aligned}$$

Furthermore,

$$\overline{f}(g(a + I + J)) = \overline{f}((a + I) \otimes (1 + J)) = a + I + J$$

$$g(\overline{f}((a+I)\otimes(b+J)) = g(ab+I+J) = (ab+I)\otimes(1+J) = b(a+I)\otimes(1+J) = (a+I)\otimes(b+J).$$

Thus, g is the inverse of f so f defines an isomorphism.

(b) Let V and W be finitely generated R modules so that $V \otimes_R W = 0$.

By the structure theorem, $V \cong R^m \oplus T(V)$ and $W \cong R^n \oplus T(W)$ where $T(V)$ and $T(W)$ are the torsion parts of V and W respectively.

Then

$$\begin{aligned}
0 &= V \otimes_R W \\
&\cong (R^m \oplus T(V)) \otimes_R (R^n \oplus T(W)) \\
&\cong (R \oplus R \oplus \cdots \oplus R \oplus T(V)) \otimes_R (R^n \oplus T(W)) \\
&\cong R \otimes_R (R^n \oplus T(W)) \oplus \cdots \oplus R \otimes_R (R^n \oplus T(W)) \oplus T(V) \otimes_R (R^n \oplus T(W)) \\
&\cong (R^n \oplus T(W)) \oplus (R^n \oplus T(W)) \oplus \cdots \oplus (R^n \oplus T(W)) \oplus T(V) \otimes_R (R^n \oplus T(W)) \\
&\cong (R^{nm} \oplus T(W)) \oplus T(V) \otimes_R (R^n \oplus T(W)) \\
&\cong (R^{nm} \oplus T(W)) \oplus (T(V) \otimes_R R^n) \oplus (T(V) \otimes_R T(W)) \\
&\cong (R^{nm} \oplus T(W)) \oplus (T(V) \otimes_R R^n) \oplus (T(V) \otimes_R T(W)) \\
&\cong (R^{nm} \oplus T(W)) \oplus [T(V)]^n \oplus (T(V) \otimes_R T(W))
\end{aligned}$$

This can only be zero if each component in the direct sum is zero.

Namely $n = m = 0$, else if $T(W) = T(V) = 0$, then $0 \cong R^{nm}$ which is a contradiction.

Finally, $V \cong T(V)$ and $W \cong T(W)$ and $T(V) \otimes_R T(W) \cong 0$.

Since $V \cong T(V)$ is finitely generated, by the structure theorem, $T(V) \cong R/(r_1) \oplus \cdots \oplus R/(r_n)$ for some ideals $(a_i) \subset R$.

Now, there is a clear homomorphism $f : R \to T(V)$ defined by $f(a) = (a + (r_1), a + (r_2), \cdots, a + (r_n))$. f will certainly be surjective.

Now, if $f(a) = 0$ then $a \in (r_1) \cap \cdots \cap (r_n)$. Namely, $a \in \mathrm{Ann}(V)$. Similarly, if $a \in \mathrm{Ann}(V)$ then $av = 0$ for all $v \in V$ and so $aR/(r_1) \oplus aR/(r_2) \oplus \cdots \oplus aR/(r_n) = 0$ so $a \in (r_1) \cap \cdots \cap (r_n)$ so $a \in \ker(f)$.

Thus,

$$T(V) \cong R/\mathrm{Ann}(V).$$

Now, finally, by (a),

$$R/(\mathrm{Ann}(V) + \mathrm{Ann}(W)) \cong R/\mathrm{Ann}(V) \otimes_R R/\mathrm{Ann}(W) \cong T(V) \otimes_R T(W) \cong 0.$$

Therefore $\mathrm{Ann}(V) + \mathrm{Ann}(W) = R$ so $1 \in \mathrm{Ann}(V) + \mathrm{Ann}(W)$ and so $\mathrm{Ann}(V)$ and $\mathrm{Ann}(W)$ are relatively prime.

✌

Problem 7. Let $g(x) = x^{12} + 5x^6 - 2x^3 + 17 \in \mathbb{Q}[x]$ and F a splitting field of $g(x)$ over $\mathbb{Q}$. Determine if $\text{Gal}(F/\mathbb{Q})$ is solvable.

Solution. Let $h(x) = x^4 + 5x^2 - 2x + 17$. Then if α is a root, $h(x)$, the third roots of α are all roots of $g(x)$. Namely, if K is the splitting field of h, then $\text{Gal}(F/K)$ is clearly solvable since every root of g to the third power is in K. Thus, it suffices to show that $\text{Gal}(K/\mathbb{Q})$ is solvable.

Now, $h'(x) = 4x^3 + 10x - 2$ which is negative for all $x \leq 1/10$ and positive for all $x \geq 1/5$. Thus, h has a minimum value somewhere between $1/10$ and $1/5$.

However, for all $\alpha \in (0, 1)$, $h(\alpha) \geq -2 + 17 > 0$. Thus, h has no real roots.

Since h has only complex roots, it has a conjugate pair of roots, $\alpha, \overline{\alpha}, \beta, \overline{\beta}$.

Note that since F is the splitting field of a separable polynomial $F/\mathbb{Q}$ is indeed Galois.

Now, $K = \mathbb{Q}(a, \overline{a}, b, \overline{b})$ is Galois over $\mathbb{Q}$. Thus, $H = \text{Gal}(F/K)$ is normal in $G = \text{Gal}(F/\mathbb{Q})$ and $\text{Gal}(K/\mathbb{Q}) = G/H$.

Now, each third rood in F clearly has minimal polynomial $x^3 - \alpha$, $x^3 - \beta$, $x^3 - \overline{\alpha}$, $x^3 - \overline{\beta}$ over K. These are irreducible since factoring would force a linear term to appear over K, and K does not contain any third roots of $\alpha, \beta, \overline{\alpha}, \overline{\beta}$.

So $[F : K] \leq 3^{12}$. Specifically, since each of these is irreducible over F, $[F : K] = 3^r$ for some $r \leq 12$.

However, then clearly H has order 3^r and so it must be solvable. This is because p-groups have non-trivial centers, and so recursively, we could obtain a subnormal chain by examining $H/Z(H)$, $H/Z(H)/Z(H/Z(H))$, etc.

Finally, $\alpha, \beta, \overline{\alpha}, \overline{\beta}$ all have minimal polynomial of degree 4 over $\mathbb{Q}$, so $[G : H] \leq 4^4$ and namely $[G : H] = 4^s = 2^{2s}$ for $s \leq 4$, so G/H is solvable.

Therefore, since H is normal in G, and H is solvable and G/H is solvable, then G is solvable.

✌