Kayla Orlinsky

Algebra Exam Spring 2012

Problem 1. Let I be an ideal of $R = \mathbb{C}[x_1, ..., x_n]$. Show that $\dim_{\mathbb{C}} R/I$ is finite if and only if I is contained in only finitely many maximal ideals of R.

Solution. $\boxed{\Longrightarrow}$ Assume R/I is a finite dimensional algebra over $\mathbb{C}$. Then R/I is artinian, since proper ideals are sub-algebras of strictly smaller degree.

Thus, if $S = \{M_1 M_2 \cdots M_k \,|\, M_i \text{ maximal ideal of } R/I\}$ is the set of finite products of maximal ideals in R/I. S is nonempty so S contains a minimal element in R/I, $M_1 M_2 \cdots M_k$. Let N be some other maximal ideal of R/I. Then $NM_1 \cdots M_k \subset M_1 \cdots M_k$ so

$$NM_1 \cdots M_k = M_1 \cdots M_k \subset N.$$

However, N is maximal and so prime, thus $M_i \subset N$ for some i. However, by maximality, $M_i = N$.

Thus, these are the only maximal ideals of R/I. By the correspondence theorem, there is a 1-to-1 correspondence between maximal ideals of R containing I and maximal ideals of R/I.

Since R/I has only finitely many maximal ideals, there are only finitely many maximal ideals of R containing I.

$\boxed{\Longleftarrow}$ Assume I is contained in only finitely many maximal ideals of R. Note that R is Noetherian by the Hilbert Basis theorem, and so all ideals are finitely generated.

Since I is contained in only finitely many maximal ideals, $V(I)$ contains only finitely many points. Namely, by Nullstellensatza,

$$\sqrt{I} \bigcap_{a \in \mathbb{C}^n} M_a \qquad \text{is a finite intersection}$$

where M_a is the maximal ideal (by Nullstellensatz) of the form $(x_1 - a_1, ..., x_n - a_n)$ for $a = (a_1, ..., a_n)$.

Thus, $\sqrt{I} = \bigcap_{i=1}^n M_{a_i}$ where $I \subset M_{a_i}$ for all i.

Since $\sqrt{I}$ is finitely generated, $\sqrt{I} = (f_1, f_2, ..., f_k)$, and for each f_i there exists m_i so $f_i^{m_i} \in I$.

Let $m = \text{lcm}\{m_i\}$. Then

$$I \subset \sqrt{I} = \bigcap_{i=1}^n M_{a_i}$$

and

$$I \supset (\sqrt{I})^m = \left(\bigcap_{i=1}^n M_{a_i}\right)^m = \bigcap_{i=1}^n M_{a_i}^m.$$

Thus, the Chinese remainder theorem, since M_{a_i} are pairwise coprime, $M_{a_i}^m$ are all pairwise coprime (since if $M_{a_i}^m + M_{a_j}^m$ is contained in some maximal ideal M, then M contains both $M_{a_i}^m$ and $M_{a_j}^m$ and so must contain both M_{a_i} and M_{a_j} which forces $M = R$).

Therefore,

$$R/\sqrt{I}^m \cong R/\cap_i M_{a_i}^m \cong R/\prod_i M_{a_i}^m \cong \prod R/M_{a_i}^m.$$

Claim 1. If F is a field and if $L = F[x_1, ..., x_n]/M$ is a field, then L is a finite field extension of F.

Proof. We proceed by induction on n.

Basecase: let $L = F[a_1]$ be a field. Then for $f(a_1) \in L$ there exists $g(a_1) \in L$ such that $f(a_1)g(a_1) = 1 \in L$ and so a_1 satisfies $h(x) = f(x)g(x) - 1$. Namely, a_1 is algebraic over F and so L is a finite field extension of F.

Assume $L = F[a_1, ..., a_k]$ is a finite field extension of F for all $k \leq n$.

Then let $L = F[a_1, ..., a_n][a_{n+1}]$. Since L is a field, by the same reasoning as the basecase, L is algebraic over $F[a_1, ..., a_n]$. However, by the inductive hypothesis, $F[a_1, ..., a_n]$ is a finite field extension of F and so

$$[L : F] = [L : F[a_1, ..., a_n]][F[a_1, ..., a_n] : F] < \infty.$$

✌

Thus, by the claim, R/M_{a_i} is a finite field extension of $\mathbb{C}$ and so namely, it is finite dimensional over $\mathbb{C}$.

Then, $R/M_{a_i}^m$ is also finite dimensional since $M_{a_i}^m \subset M_{a_i}$ so we can inject $R/M_{a_i}^m \hookrightarrow R/M_{a_i}$ which is finite dimensional, so $R/M_{a_i}^m$ is finite dimensional, and so $R/\sqrt{I}^m$ is finite dimensional since it is a product of finite dimensional algebras.

Finally,

$$R/I \cong (R/\sqrt{I}^m)/(I/\sqrt{I}^m)$$

is a quotient of a finite dimensional algebra, and so R/I is a finite dimensional $\mathbb{C}$-algebra.

✌

Problem 2. . If G is a group with $|G| = 7^2 \cdot 11^2 \cdot 19$, show that G must be abelian and describe the possible structures of G.

Solution. By Sylow, $n_7 \equiv 1 \mod 7$ and $n_7 | 11^2 \cdot 19$. Since $11^2 \equiv 2 \mod 7$, $11 \cdot 19 \equiv 6 \mod 7$, $11^2 \cdot 19 \equiv 3 \mod 7$, $n_7 = 1$.

Thus, G has a normal Sylow 7-subgroup P_7.

Thus, $H = P_7 P_{11}$ is a subgroup of G where P_{11} is a Sylow 11-subgroup of G.

Now, let $X = G/H$ the set of let cosets of H. Then $|X| = 19$.

Let G act on X by left multplication. Then this defines a homomorphism

$$\begin{aligned} \varphi : G &\to S_{|X|} = S_{19} \\ a &\mapsto \sigma_a : X \to X \qquad \sigma_a(gH) = agH \end{aligned}$$

Note that φ is not an embedding since 11^2 does not divide $19!$. Therefore, 11 divides $|\ker(\varphi)|$ and so there exists an element $x \in \ker(\varphi)$ of order 11.

Now, if $\varphi(a) = \text{Id}$, then $agH = gH$ for all $g \in G$ so $a \in gHg^{-1}$ for all $g \in G$.

Namely, $\ker(\varphi) = \bigcap\limits_{g \in G} gHg^{-1}$. Note also that P_7 is normal in G and so because $gP_7g^{-1} = P_7 \subset gHg^{-1}$ for all g.

Therefore,

$$|\ker(\varphi)| = \left| \bigcap_{g \in G} gHg^{-1} \right| \geq 7^2 \cdot 11.$$

Namely, $|\varphi(G)| = 11 \cdot 19$, or 19, namely $\varphi(G)$ is abelian by Sylow.

However, G acts transitively on X, since for $gH, aH \in X$,

$$gH = ga^{-1}aH = ga^{-1}(aH) = g_0(aH) \qquad g_0 = ga^{-1}.$$

Therefore, $\varphi(G)$, which is necessarily abelian based on its order, is a transitive subgroup of S_{19}, and so it has order 19. If the order were larger, then there would exist $x = \varphi(a)(1) = \varphi(b)(1)$ and $\varphi(a)(y) \neq \varphi(b)(y)$. Thus, by transitivity, there is $\varphi(c)(x) = y$, then

$$\varphi(c)\varphi(a)\varphi(c)\varphi(b)(1) = \varphi(c)\varphi(a)\varphi(c)(x) = \varphi(c)\varphi(a)(y)$$

and

$$\varphi(c)\varphi(b)\varphi(c)\varphi(a)(1) = \varphi(c)\varphi(b)\varphi(c)(x) = \varphi(c)\varphi(b)(y)$$

which cannot be equal to $\varphi(b)(y) \neq \varphi(a)(y)$ which contradicts that $\varphi(G)$ is abelian.

Thus, $|\varphi(G)| = 19$ so $|\ker(\varphi)| = |H|$ so $\ker(\varphi) = H$ and so H is normal in G. Therefore, because H has a normal Sylow 11-subgroup (since $n_{11}|49$ and $n_{11} \equiv 1 \mod 11$ in H, $n_{11} = 1$)

and since normal Sylow subgroups of normal subgroups are normal in the whole group (see **Fall 2011: Problem 5 Claim 3**), G has a normal Sylow 11-subgroup.

Now, by the recognizing of semi-direct products theorem, if G is not abelian then it is a semi-direct product of its Sylow subgroups.

However, $\text{Aut}(P_7P_{11}) \cong \text{Aut}(P_7) \times \text{Aut}(P_{11})$ since 11 and 7 are coprime. Thus, depending on whether $P_7 \cong \mathbb{Z}_7 \times \mathbb{Z}_7$ or $\mathbb{Z}_{49}$ we have that

$$\text{Aut}(P_7) \cong \mathbb{Z}_{49-7} = \mathbb{Z}_{42} \qquad \text{Aut}(P_7) \cong GL_2(\mathbb{F}_7).$$

In either case, $|\text{Aut}(P_7)| = 42$ or $(7^2-1)(7^2-7) = 48 \cdot 42$ and 19 does not divide either of these.

Similarly, $\text{Aut}(P_{11})$ has order $11^2 - 11 = 110$ or $(11^2-1)(11^2-11) = 120 \cdot 110$, and again there are no elements of order 19 to choose from.

Therefore, any homomorphism $\varphi : P_{19} \to \text{Aut}(P_7P_{11})$ will be trivial and so the only possible structure for G is as an abelian group.

There are 4 possible abelian structures for G.

$$\mathbb{Z}_{7^2} \times \mathbb{Z}_{11^2} \times \mathbb{Z}_{19}$$

$$\mathbb{Z}_7 \times \mathbb{Z}_7 \times \mathbb{Z}_{11^2} \times \mathbb{Z}_{19}$$

$$\mathbb{Z}_{7^2} \times \mathbb{Z}_{11} \times \mathbb{Z}_{11} \times \mathbb{Z}_{19}$$

$$\mathbb{Z}_7 \times \mathbb{Z}_7 \times \mathbb{Z}_{11} \times \mathbb{Z}_{11} \times \mathbb{Z}_{19}$$

✌

Problem 3. Let F be a finite field and G a finite group with $\text{GCD}\{charF, |G|\} = 1$. The group algebra $F[G]$ is an algebra over F with G as an F-basis, elements $\alpha = \sum_G a_g g$ for $a_g \in G$, and multiplication that extends $ag \cdot bh = ab \cdot gh$. Show that any $x \in F[G]$ that is not a zero left divisor (i.e. if $xy = 0$ for $y \in F[G]$ then $y = 0$) must be invertible in $F[G]$.

Solution. Let $x \in F[G]$ be not a zero left divisor. Then because $F[G]$ is a finite field and G is a finite group, $F[G]$ is a finite dimensional F-algebra and so it is artinian (both left and right artinian) as an F-algebra.

Namely, we can construct a decreasing chain of left ideals

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

which must terminate after a finite number of steps. Namely, there exists n so $(x^m) = (x^n)$ for all $m \geq n$.

Thus, $(x^{n+1}) = (x^n)$ so there exists $y \in F[G]$ such that $x^n = yx^{n+1}$. Namely, $(1-yx)x^n = 0$. Since x is not a left-zero divisor, $(1 - yx)x^{n-1} = 0$, and recursivley we obtain that $(1 - yx) = 0$ so $yx = 1$. Namely, x has a left inverse in G.

Now, assume x is a right zero-divisor. Then there exists $a \in F[G]$ so $xa = 0$. Thus,

$$(yx)a = 1a = a \qquad y(xa) = y(0) = 0 \implies a = 0.$$

Therefore, x is not a right-zero divisor, and since $F[G]$ is right artinian we could preform the same reasoning as before on $(x), (x^2), ...$ as right ideals to obtain that x has a right inverse z.

Now, since

$$(yx)z = 1z = z \qquad y(xz) = y1 = y$$

we have that $y = z$ and so y is a 2-sided inverse for x. ✌

Problem 4. If $p(x) = x^8 + 2x^6 + 3x^4 + 2x^2 + 1 \in \mathbb{Q}[x]$ and if $\mathbb{Q} \subset M \subset \mathbb{C}$ is a splitting field for $p(x)$ over $\mathbb{Q}$, argue that $\mathrm{Gal}(M/\mathbb{Q})$ is solvable.

Solution. Let $u = x^2$ and $h(u) = u^4 + 2u^3 + 3u^2 + 2u + 1$. Then the zeros of of $p(x)$ are precisely the square roots of the zeros of $h(u)$. Namely, if L is the splitting field of $h(u)$ over $\mathbb{Q}$ then M/L will certainly be a radical extension so we need only check $L/\mathbb{Q}$.

Now, $h'(u) = 4u^3 + 6u^3 + 6u + 2$ and $h'(u) < 0$ for all $u \le -1/3$ and $h'(u) > 0$ for all $u \ge 0$. However, for any $\alpha \in (-1/3, 0)$,

$$h(\alpha) = \alpha^4 + 2\alpha^3 + 3\alpha^2 + 2\alpha + 1 > -\frac{2}{9} - \frac{2}{3} + 1 = -\frac{8}{9} + 1 > 0.$$

Therefore, h has no real roots, and namely no rational roots. Thus, h has a pair of complex conjugate roots, $\alpha, \overline{\alpha}, \beta, \overline{\beta}$.

Therefore, L is the splitting field of a separable polynomial over $\mathbb{Q}$ and so L is Galois over $\mathbb{Q}$.

Since $[L : \mathbb{Q}] \le 4!$, and $\mathrm{Gal}(L/\mathbb{Q}) \hookrightarrow S_4$ which is solvable, we have that $\mathrm{Gal}(L/\mathbb{Q})$ is solvable since subgroups of solvable groups are solvable.

Finally, if $G = \mathrm{Gal}(M/\mathbb{Q})$, then by the fundamental theorem of Galois theory, $H = \mathrm{Gal}(M/L)$ is normal in G and $G/H = \mathrm{Gal}(L/\mathbb{Q})$. Namely, since H is normal in G and is solvable (as we already discussed M/L is a radical extensions) and G/H is solvable, we have that G is solvable. ✌

Problem 5. Let R be a commutative ring with 1 and let $x_1, ..., x_n \in R$ so that $x_1y_1 + \cdots + x_ny_n = 1$ for some $y_i \in R$. Let $A = \{(r_1, ..., r_n) \in R^n \,|\, x_1r_1 + \cdots + x_nr_n = 0\}$. Show that $R^n \cong_R A \oplus R$, that A has n generators, and that when $R = F[x]$ for F a field then A_R is free of rank $n - 1$.

Solution. Let

$$\begin{aligned} \varphi : R^n &\to R \\ (r_1, ..., r_n) &\mapsto x_1r_1 + \cdots + x_nr_n \end{aligned}$$

Then φ is an R-module homomorphism and is surjective since $(y_1, ..., y_n) \mapsto 1$.

Clearly $\ker(\varphi) = A$, thus we have a short exact sequence

$$0 \longrightarrow A \longrightarrow R^n \longrightarrow R \longrightarrow 0$$

and since R is a projective R-module (both left and right because R is commutative), this implies that

$$R^n \cong R \oplus A.$$

Since $R = x_1R + x_2R + \cdots + x_nR$, $R^n = (x_1R + x_2R + \cdots + x_nR)^n$ and since A is a submodule of R^n, A has less than or equal to n generators.

However, because $R^n/A \cong R$ is cyclic, A has at least n generators.

Thus, A has exactly n generators.

When $R = F[x]$, then R is a PID and so because A is finitely generated, by the structure theorem, A is a direct sum of its free and torsion parts.

Namely, we have that $A \cong R^a \oplus T(A)$ where $T(A)$ is the torsion part of A.

Now, since

$$R^n \cong R \oplus R^a \oplus T(A) \cong R^{a+1} \oplus T(A)$$

it must be that $a + 1 = n$ so $a = n - 1$ and $T(A) = 0$.

Thus, A is a free R-module of rank $n - 1$. ✌

Problem 6. For p a prime let F_p be the field of p elements and K an extension field of F_p of dimension 72.

(a) Describe the possible structures of $\text{Gal}(K/F_p)$.

(b) If $g(x) \in F_p[x]$ is irreduicble of degree 72, argue that K is a splitting field of $g(x)$ over F_p.

(c) Which integers $d > 0$ have irreducibles in $F_p[x]$ of degree d that split in K?

Solution.

(a) Since K has $q = p^{72}$ elements, K is the splitting field of $x^q - x$,which is separable over F_p. Thus, K/F_p is Galois.

Since Galois extensions over finite fields are always cyclic extensions, $\text{Gal}(K/F_p) \cong \mathbb{Z}_{72}$.

(b) If $g(x) \in F_p[x]$ is irreduicble of degree 72, and α is a root of $g(x)$, then $[F_p(\alpha) : F_p] = 72 = [K : F_p]$. Therefore, since finite fields of the same order are isomorphic, $K = F_p(\alpha)$ and so $\alpha \in K$.

(c) If $d|72$ then by the same reasoning, any polynomial of degree d will split completely in K.

✌