1 Spring 2012: Algebra Graduate Exam

1.1 Problem 1.

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

Proof. $\square$

1.2 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.

Proof. We'll start by using Sylow's theorems. Firstly, let r_p denote the number of Sylow p-subgroups. Since p divides $|G|$,

$$\begin{aligned} r_{19} &\in \{1, 7, 7^2, 11, 11 \cdot 7, 11 \cdot 7^2, 11^2, 11^2 \cdot 7, 11^2 \cdot 7^2\}, \\ r_{11} &\in \{1, 7, 7^2, 19, 19 \cdot 7, 19 \cdot 7^2\}, \\ r_7 &\in \{1, 11, 11^2, 19, 19 \cdot 11, 19 \cdot 11^2\}. \end{aligned}$$

Since $r_p \cong 1 \bmod p$, we can further refine this to

$$\begin{aligned} r_{19} &= 1, \\ r_{11} &\in \{1, 19 \cdot 7\}, \\ r_7 &= 1. \end{aligned}$$

This means that we have unique subgroups H_{19} and H_7 of orders 19 and 7 respectively. Since H_7 and H_{19} are unique and thus normal, the product of H_7 and H_{19} forms a normal subgroup, call it N. Since $H_7 \cap H_{19} = \{e\}$, $H_7 H_{19} \cong H_7 \times H_{19}$, where H_{19} is abelian because it is cyclic, and H_7 is abelian because all groups of order p^2 are abelian. Thus $N \cong \mathbb{Z}_7 \times \mathbb{Z}_7 \times \mathbb{Z}_{19}$ or $N \cong \mathbb{Z}_{49} \times \mathbb{Z}_{19}$.

Since N and H_{11} are complementary, that is $N \cap H_{11} = \{e\}$ and $|N||H_{11}| = |G|$, G can be realized as the semidirect product of N and H_{11}

$$G = N \rtimes H_{11}.$$

Thus it is enough to consider the possible structures of the semidirect product.

Case 1. Assume $N \cong \mathbb{Z}_7 \times \mathbb{Z}_7 \times \mathbb{Z}_{19}$. Consider homomorphisms $\varphi \colon H_{11} \to \mathrm{Aut}(N)$, noting that

$$\mathrm{Aut}(N) \cong \mathrm{Aut}(\mathbb{Z}_7 \times \mathbb{Z}_7 \times \mathbb{Z}_{19}) \cong \mathrm{Aut}(\mathbb{Z}_7 \times \mathbb{Z}_7) \times \mathrm{Aut}(\mathbb{Z}_{19}) \cong \underbrace{\mathrm{Aut}(\mathbb{Z}_7 \times \mathbb{Z}_7)}_{\text{order } 48 \cdot 42} \times \mathbb{Z}_{18}.$$

Since $\gcd(11, 48 \cdot 42 \cdot 18) = 1$, the only homomorphism is trivial. So the semidirect product is direct

$$G \cong \mathbb{Z}_7 \times \mathbb{Z}_7 \times \mathbb{Z}_{19} \times H_{11}$$

Case 2. Assume $N \cong \mathbb{Z}_{49} \times \mathbb{Z}_{19}$. Consider homomorphisms $\varphi \colon H_{11} \to \mathrm{Aut}(N)$, noting that

$$\mathrm{Aut}(N) \cong \mathrm{Aut}(\mathbb{Z}_{49} \times \mathbb{Z}_{19}) \cong \mathrm{Aut}(\mathbb{Z}_{49}) \times \mathrm{Aut}(\mathbb{Z}_{19}) \cong \underbrace{\mathrm{Aut}(\mathbb{Z}_7 \times \mathbb{Z}_7)}_{\text{order } 7 \cdot 6} \times \mathbb{Z}_{18}.$$

Since $\gcd(11, 7 \cdot 6 \cdot 18) = 1$, the only homomorphism is trivial. So the semidirect product is direct

$$G \cong \mathbb{Z}_{49} \times \mathbb{Z}_{19} \times H_{11}$$

Since $|H_{11}| = 11^2$, it is abelian, so by the fundamental theorem of abelian groups, G is isomorphic to

$$\begin{aligned} &\mathbb{Z}_7 \times \mathbb{Z}_7 \times \mathbb{Z}_{11} \times \mathbb{Z}_{11} \times \mathbb{Z}_{19}, \\ &\mathbb{Z}_7 \times \mathbb{Z}_7 \times \mathbb{Z}_{121} \times \mathbb{Z}_{19}, \\ &\mathbb{Z}_{49} \times \mathbb{Z}_{11} \times \mathbb{Z}_{11} \times \mathbb{Z}_{19}, \qquad \text{or} \\ &\mathbb{Z}_{49} \times \mathbb{Z}_{121} \times \mathbb{Z}_{19}. \end{aligned}$$

□

1.3 Problem 3.

Let F be a finite field and G a finite group with $\gcd\{\operatorname{char} F, |G|\} = 1$. The group algebra $F[G]$ is an algebra over F with G as an F-basis, elements $\alpha = \sum_G a_g g$ for $g \in F$, and multiplication that extends $ag \cdot bh = ab \cdot gh$. Show that any $x \in F[G]$ that is not a zero left divisor must be invertible in $F[G]$.

Note: Since x is not a zero left divisor, if $xy = 0$ for $y \in F[G]$ then $y = 0$.

Proof. Since $\operatorname{char} F$ does not divide $|G|$, by Mashke's Theorem, $F[G]$ is semisimple, so by the Artin-Wedderburn theorem,

$$F[G] \cong M_{n_1}(D_1) \times M_{n_2}(D_2) \times \ldots \times M_{n_k}(D_k)$$

where $M_{n_i}(D_i)$ is an n_i-by-n_i matrix ring over a division ring D_i.

Thus any $\alpha = \sum_{g \in G} a_g g \in F[G]$ maps under the isomorphism to

$$\varphi(\alpha) = (a_1, a_2, \ldots, a_k) \in M_{n_1}(D_1) \times \ldots \times M_{n_k}(D_k).$$

Now suppose for the sake of contradiction that some a_i is not invertible for some i; without loss of generality, say that $i = 1$. Then there exists some $b \neq 0 \in M_{n_1}(D_1)$ such that $a_1 b = 0$ (why?), and

$$(a_1, a_2, \ldots, a_k) \cdot (b, 0, 0, \ldots, 0) = (\underbrace{a_1 b}_{0}, 0, 0, \ldots, 0).$$

Therefore $\varphi^{-1}(a_1, a_2, \ldots, a_k) = x$ is a left divisor.

Thus in order for x not to be a left divisor, all a_i must be invertible. Thus $x^{-1} = \varphi^{-1}(a_1^{-1}, a_2^{-1}, \ldots, a_k^{-1})$. □

1.4 Problem 4.

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

Proof. Let $q(y) = y^4 + 2y^3 + 3y^2 + 2y + 1$ so that $q(x^2) = p(x)$. Since $\deg(q) = 4$, q is solvable by radicals with roots $\{a_1, a_2, a_3, a_4\}$ expressible as radicals. Thus p is also solvable by radicals with roots $\{\pm\sqrt{a_1}, \pm\sqrt{a_2}, \pm\sqrt{a_3}, \pm\sqrt{a_4}\}$. $\square$

1.5 Problem 5.

Let R be a commutative ring with 1 and let $x_1, \ldots, x_n \in R$ so that $x_1y_1 + \ldots + x_ny_n = 1$ for some $y_j \in R$. Let $A = \{(r_1, r_2, \ldots, r_n) \in R^n \mid x_1r_1 + \ldots + x_nr_n = 0\}$. Show that

(i) $R^n \cong_R A \oplus R$,

(ii) A has n generators, and

(iii) when $R = F[x]$ for F a field, then A_R is free of rank $n-1$.

Proof. First consider the map $\varphi\colon R^n \to R$ that sends $(r_1, \ldots, r_n) \mapsto x_1r_1 + \ldots + x_nr_n$ so that $\varphi(y_1, \ldots, y_n) = 1$ and thus is surjective. Notice also that $\ker(\varphi) = A$. So the short exact sequence splits:

$$0 \to A \hookrightarrow R^n \twoheadrightarrow R \to 0$$

(i) Since R, as a module over itself, is free and thus projective, so $R^n \cong_R A \oplus R$.

(ii) (?)

(iii) If $R = F[x]$, then R is a PID. Thus by the structure theorem for finitely generated modules over a PID,

$$A \cong T(A) \oplus R^k$$

and since $R^n \cong A \oplus R = T(A) \oplus R^{k+1}$, $T(A) \cong 0$ and $k = n-1$, so $\text{rank}(A) = \text{rank}(R^{n-1}) = n-1$.

□

1.6 Problem 6.

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

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

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

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

Proof. $\square$