Kayla Orlinsky

Algebra Exam Spring 2014

Problem 1. Let L be a Galois extension of a field F with $\mathrm{Gal}(L/F) \cong D_{10}$, the dihedral group of order 10. How many subfields $F \subset M \subset L$ are there, what are their dimensions over F, and how many are Galois over F?

Solution. $|D_{10}| = 10 = 2 \cdot 5$. Thus, by Sylow, $n_5 \equiv 1 \mod 5$ and $n_5 | 2$ so $n_5 = 1$. Thus, D_{10} has one Sylow 5-subgroup which is normal. Since D_{10} is not abelian, $n_2 \neq 1$. Thus, $n_2 \equiv 1 \mod 2$ and $n_2 | 5$ so $n_2 = 5$.

There is the trivial subgroup $\{e\}$ which corresponds to the basefield F which is trivially galois over itself.

There are 5 subgroups P_i $i = 1, ..., 5$ of order 2, which are not normal in G. Thus, there are 5 intermediate fields $F \subset M_i \subset L$ $i = 1, ..., 5$, such that $|P_i| = [L : M_i] = 2$ so $[M_i : F] = 5$ and M_i/F is not a galois extension for $i = 1, ..., 5$.

There is 1 normal subgroup of order 5 Q. Thus, there is one intermediate field $F \subset K \subset L$ with $|Q| = 5 = [L : K]$ and $[K : F] = 2$ and K/F is a galois extension.

Finally, there is the top field L which corresponds to $D_{10} = \mathrm{Gal}(L/F)$ which is galois over F and $[L : F] = 10$. ✌

Problem 2. Up to isomorphism, using direct and semi-direct products, describe the possible structures of a group of order $5 \cdot 11 \cdot 61$.

Solution. Let G be a group of order $5 \cdot 11 \cdot 61$. Then by Sylow, $n_{61} \equiv 1 \mod 61$ and $n_{61} | 5 \cdot 11$. Thus, $n_{61} = 1$. Also, $n_{11} \equiv 1 \mod 11$ and $n_{11} | 5 \cdot 61$. Since $61 \not\equiv 1 \mod 11$ and $305 \equiv 8 \mod 11$, we have that $n_{11} = 1$ as well.

Therefore, G has a normal Sylow 11-subgroup P_{11} and a normal Sylow 61-subgroup P_{61}.

Abelian If G also has a normal Sylow 5-subgroup P_5, then G is abelian and

$$G \cong \mathbb{Z}_{3355}.$$

Else, we have by the recognizing of semi-direct products theorem that G is a semi-direct product of its Sylow subgroups.

There are 3 possible homomorphisms to check.

$\varphi : P_5 P_{11} \to \text{Aut}(P_{61})$ Since P_{11} is normal, $P_5 P_{11}$ is a subgroup of G. Let $\varphi : P_5 P_{11} \to \text{Aut}(P_{61}) \cong \mathbb{Z}_{60}$ be a homomorphism.

Let $P_5 \cong \langle a \rangle$, $P_{11} \cong \langle b \rangle$, $P_{61} \cong \langle c \rangle$.

Then because $\mathbb{Z}_{60}$ has no elements of order 11, φ is determined by where it sends P_5. Since $\mathbb{Z}_{60}$ is abelian, it has one normal Sylow 5-subgroup so $\varphi(a)$ will be some generator of the Sylow 5-subgroup of $\mathbb{Z}_{60}$. Namely, $\varphi_1(a)$ will be some power of $\varphi_2(a)$ for any two homomorphisms φ_1 and φ_2. Therefore, φ_1 and φ_2 will generate ismorophic semi-direct products since $a \mapsto a^i$ is an isomorphism of P_5 for $i = 1, ..., 4$.

Thus, we need to only find one automorphism of P_{61} of order 5.

The map $\sigma : c \mapsto c^9$ has order 5. This defines multiplication on G by $bcb^{-1} = \varphi(b)(c) = c$ and $aca^{-1} = \varphi(a)(c) = c^9$.

Thus,

$$G \cong \langle a, b, c \,|\, a^5 = b^{11} = c^{61} = 1, ab = ba, bc = cb, ac = c^9 a \rangle$$

$\varphi : P_5 P_{61} \to \text{Aut}(P_{11})$ $\varphi : P_5 P_{61} \to \text{Aut}(P_{11}) \cong \mathbb{Z}_{10}$.

Again, $\mathbb{Z}_{10}$ has one Sylow 5-subgroup and no elements of order 61 so again, we will obtain only one unique structure defined by $\varphi(a)$ having order 5.

Since $\tau : c \mapsto c^3$ has order 5 we have

$$G \cong \langle a, b, c \,|\, a^5 = b^{11} = c^{61} = 1, ac = ca, bc = cb, ab = b^3 a \rangle$$

$\varphi : P_5 \to \text{Aut}(P_{11} P_{61})$ Since 11 and 61 are coprime, $\text{Aut}(P_{11} P_{61}) \cong \text{Aut}(P_{11}) \times \text{Aut}(P_{61})$.

Now, $\varphi(a) = (\sigma, \text{Id}), (\text{Id}, \tau)$ will define the same structures that we have already found. Namely, the only new structure would be defined by $\varphi(a) = (\sigma, \tau)$.

Thus, the final structure is

$$G \cong \langle a, b, c \,|\, a^5 = b^{11} = c^{61} = 1, ab = b^3a, bc = cb, ac = c^9a \rangle$$

Thus, there are four possible group structures for G.

$$\mathbb{Z}_{3355}$$

$$\langle a, b, c \,|\, a^5 = b^{11} = c^{61} = 1, ab = ba, bc = cb, ac = c^9a \rangle$$

$$\langle a, b, c \,|\, a^5 = b^{11} = c^{61} = 1, ac = ca, bc = cb, ab = b^3a \rangle$$

$$\langle a, b, c \,|\, a^5 = b^{11} = c^{61} = 1, bc = cb, ab = b^3a, ac = c^9a \rangle$$

✌

Problem 3. Let I be a nonzero ideal of $R = \mathbb{C}[x_1, ..., x_n]$. Show that R/I is a finite dimensional algebra over $\mathbb{C}$ if and only if I is contained in only finitely many maximal ideals of R.

Solution. This is the same question as **Spring 2012: Problem 1**. We provide the same proof here as we did there. $\boxed{\implies}$ 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 $S = \{M_1M_2 \cdots M_k \,|\, M_i \text{ maximal ideal of } R/I\}$ is the set of finite products of maximal ideals in R/I. S is nonempty so S contains a minimal element in R/I, $M_1M_2 \cdots M_k$. 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.

$\boxed{\impliedby}$ 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 4. Let R be a commutative ring with 1, and M a noetherian R-module. For N a noetherian R module show that $M \otimes_R N$ is a noetherian R-module. When N is an artinian R module show that $M \otimes_R N$ is an artinian R module.

Solution. Since M is noetherian, M is finitely generated. Namely, $M = m_1 R + \cdots + m_n R$ for some $m_1, ..., m_n \in M$.

Thus, we can define a module isomorphism

$$\begin{aligned} f : M &\to R^n \\ m_i &\mapsto (0, 0, ..., 0, 1, 0, ..., 0) \qquad i^{\text{th}}\text{-position} \end{aligned}$$

Therefore, we have a short exact sequence

$$0 \longrightarrow R^n \longrightarrow M \longrightarrow 0$$

and since tensor products are right-regular,

$$R^n \otimes_R N \longrightarrow M \otimes_R N \longrightarrow 0$$

and so

$$R^n \otimes_R N \cong N^n \text{ (direct sum) } \cong M \otimes_R N.$$

Since N is noetherian, a direct sum of n copies of N is noetherian and so $M \otimes_R N$ is noetherian.

Similarly, if N is artinian, a direct sum of n copies of N is artinian and so $M \otimes_R N$ is artinian.

✌

Problem 5. For $n \geq 5$ show that the symmetric group S_n cannot have a subgroup H with $3 \leq [S_n : H] < n$ ($[S_n : H]$ is the index of H in S_n).

Solution. Note that A_n is always a subgroup of S_n of index 2.

Let H be a subgroup of S_n such that $2 < [S_n : H] = k < n$. Then let S_n act on $X = S_n/H$ the set of left cosets (not necessarily a group) by left multiplication.

This defines a map

$$\begin{aligned} \varphi : S_n &\to S_{|X|} = S_k \\ a &\mapsto \sigma_a \end{aligned}$$

where $\sigma_a : X \to X$ is defined by $\sigma_a(bH) = abH$.

Now, if $a \in \ker(\varphi)$ then $abH = bH$ for all b. Then $abh = bh'$ for $h, h' \in H$ so $a = bh'h^{-1}b^{-1} \in bHb^{-1}$.

Thus,

$$a \in \bigcap_{b \in S_n} bHb^{-1} \subset H.$$

Therefore, $\ker(\varphi) \subset H$. However, the only normal subgroups of S_n for $n \geq 5$ are the trivial one, S_n itself, or S_n.

Since $|H| < |A_n|$, $|\ker(\varphi)| \neq n!/2, n!$, so the kernel is trivial.

However, then S_n has an isomorphic copy inside S_k, which is not possible since $k < n$ so $k! < n!$.

Thus, H cannot exist. ✌

Problem 6. Let R be the group algebra $\mathbb{C}[S_3]$. How many nonisomorphic, irreducible, left modules does R have and why?

Solution. First, by classification theorems for group algebras, $\mathbb{C}[S_3]$ is semi-simple and has 3 simple components because S_3 has 3 conjugacy classes.

Furthermore, $|S_3| = 6 = n_1^2 + n_2^2 + n_3^2$ by Mashke's theorem where n_i correspond to the simple components $M_{n_i}(\mathbb{C})$ comprising $\mathbb{C}[S_3]$.

Therefore, if $n_3 \leq 2$, and since S_3 is not abelian, not all the n_i are 1. Thus, if $n_3 = 2$, then $6 = n_1^2 + n_2^2 + 4$ so $n_1 = n_2 = 1$.

Therefore,

$$\mathbb{C}[S_3] \cong \mathbb{C}^2 \oplus M_2(\mathbb{C}).$$

Since the number of non-isomorphic simple left R-module is exactly the number of simple components in the decomposition, R has 3 non-isomorphic simple left R-modules.

***Although it was not asked, the simple left $\mathbb{C}[S_3]$-modules are exactly $\mathbb{C}[S_3]/I$ for some maximal left ideal I.
Since maximal ideals of $\mathbb{C}[S_3]$ are

$$\begin{aligned} I_1 &= (0) \oplus \mathbb{C} \oplus M_2(\mathbb{C}) \\ I_2 &= \mathbb{C} \oplus (0) \oplus M_2(\mathbb{C}) \\ I_3 &= \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C}^2 \end{aligned}$$

since the maximal left ideal of $\mathbb{C}$ is (0) and the maximal left ideals of $M_2(\mathbb{C})$ are the column spaces, namely, $\mathbb{C}^2$.
Therefore, the non-isomorphic simple left $\mathbb{C}[S_3]$-modules are

$$M_1 \cong \mathbb{C} \text{ (first component)}, \qquad M_2 \cong \mathbb{C} \text{ (second component)}, \qquad M_3 \cong \mathbb{C}^2.$$

✌

Problem 7. Let each $g_1(x), g_2(x), ..., g_n(x) \in \mathbb{Q}[x]$ be irreducible of degree four and let L be a splitting field over $\mathbb{Q}$ for $\{g_1(x), ..., g_n(x)\}$. Show there is an extension field M of L that is a radical extension of $\mathbb{Q}$.

Solution. Since the g_i are irreducible over $\mathbb{Q}$, they are separable.

Let L_i be the splitting field of g_i over $\mathbb{Q}$.

Then since L_i is the splitting field of a separable polynomial, it is a Galois extension of $\mathbb{Q}$. Since $G_i = \text{Gal}(L_i/\mathbb{Q})$ is a subgroup of S_4 (because $|G| = [L_i/\mathbb{Q}] \leq 4!$ so G embeds into S_4) which is solvable, and since subgroups of solvable groups are solvable, G_i is solvable.

Thus, $g_i(x)$ is solvable by radicals and L_i is a radical extension.

Therefore, we obtain a chain,

$$\mathbb{Q} \subset L_1 \subset L_1 L_2 \subset \cdots \subset L_1 L_2 \ldots L_n = M$$

where each product of the L_i is radical over $\mathbb{Q}$ and so M is certainly a radical extension.

Therefore, $L \subset L_1 \cdots L_n = M$ is contained in a radical extension of $\mathbb{Q}$. ✌