Kayla Orlinsky

Algebra Exam Fall 2012

Problem 1. Use Sylow's theorems directly to find, up to isomorphism, all possible structures of groups of order $5 \cdot 7 \cdot 23$.

Solution. Let G be a group of order $5 \cdot 7 \cdot 23$.

By Sylow, $n_{23} \equiv 1 \mod 23$ and $n_{23}|35$, so $n_{23} = 1$.

Similarly, $n_7 \equiv 1 \mod 7$ and $n_7|5 \cdot 23$. Since $5 \cdot 23 = 115 \equiv 3 \mod 7$, we have that $n_7 = 1$.

$\boxed{\text{Abelian}}$ If G also has a normal Sylow 5 subgroup, then G is abelian and isomorphic to $\mathbb{Z}_5 \times \mathbb{Z}_7 \times \mathbb{Z}_{23}$.

If G does not have a normal Sylow 5-subgroup, then by the recognizing semi-direct products theorem, G is isomorphic to a semi direct product of its Sylow subgroups.

$\boxed{\varphi : P_5 \to \text{Aut}(P_7P_{23})}$ Let P_5, P_7, P_{23} be Sylow $5, 7, 23$-subgroups of G respectively.

Then if we have a homomorphism, $\varphi : P_5 \to \text{Aut}(P_7P_{23}) \cong \text{Aut}(P_7)\times\text{Aut}(P_{23}) \cong \mathbb{Z}_6\times\mathbb{Z}_{22}$ (since 7 and 23 are coprime), we have that φ must be trivial since neither group has any elements of order 5.

$\boxed{\varphi : P_5P_7 \to \text{Aut}(P_{23})}$ If $\varphi : P_5P_7 \to \text{Aut}(P_{23}) \cong \mathbb{Z}_{22}$ is a homomorphism, then φ must be again trivial since $\mathbb{Z}_{22}$ has no elements of order 5 or order 7.

$\boxed{\varphi : P_5P_{23} \to \text{Aut}(P_7)}$ if $\varphi : P_5P_{23} \to \text{Aut}(P_7) \cong \mathbb{Z}_6$ is a homomorphism, then φ is again trivial since there are no elements of order 5 or order 23 in $\mathbb{Z}_6$.

Thus, there is only one group of order $5 \cdot 7 \cdot 23$,

$$\boxed{\mathbb{Z}_5 \times \mathbb{Z}_7 \times \mathbb{Z}_{23}}$$

✌

Problem 2. Let A, B, C be finitely generated $F[x] = R$ modules, for F a field, with C torsion free. Show that $A \otimes_R C \cong B \otimes_R C$ implies that $A \cong B$. Show by example that this conclusion can fail when C is not torsion free.

Solution. Because F is a field, $F[x]$ is a PID, so because A, B, C are finitely generated, by the structure theorem, we can write each as a direct sum of its free and torsion part.

Namely, because C is torsion free, C is a free module so $C \cong R^n$ for some n.

Thus,

$$A \otimes_R C \cong A \otimes_R R^n \cong A^n \cong B \otimes_R C \cong B^n.$$

Since $A^n \cong B^n$ implies that the free parts and torsion parts of A^n and B^n are both isomorphic. Namely, if $A \cong R^a \oplus T(A)$ and $B \cong R^b \oplus T(B)$ with $T(A)$ and $T(B)$ the torsion parts of A and B respectively.

Then there exists a chain of nonzero ideals $(a_1) \subset (a_2) \subset \cdots \subset (a_k) \subset A$ and $(b_1) \subset (b_2) \subset \cdots \subset (b_l) \subset B$ with

$$T(A) \cong \bigoplus_{i=1}^{k} R/(a_i) \qquad T(B) \cong \bigoplus_{j=1}^{l} R/(b_i).$$

Now, since $A^n \cong B^n$, then

$$R^{an} \cong R^{bn} \implies a = b$$

and

$$(T(A))^n \cong (R/(a_1))^n \oplus \cdots \oplus (R/(a_k))^n \cong (R/(b_1))^n \oplus \cdots \oplus (R/(b_l))^n.$$

Therefore, each component, $R/(a_i)$ of $T(A)$ must be represented in the decomposition for $T(B)$ so $T(A) \cong T(B)$.

Thus, $A \cong B$.

Now, assume C has nontrivial torsion part. Let $A = B \oplus \text{Ann}(C)$. Then

$$A \otimes_R C = (B \oplus \text{Ann}(C)) \otimes_R C \cong (B \otimes_R C) \oplus (\text{Ann}(C) \otimes_R C) \cong B \otimes_R C$$

since $\text{Ann}(C) \subset R$ and so each element transfers over and kills C. However, since $\text{Ann}(C)$ is nonzero, $A \ncong B$. ✌

Problem 3. Working in the polynomial ring $\mathbb{C}[x,y]$, show that some power of $(x+y)(x^2+y^4-2)$ is in (x^3+y^3, y^3+xy).

Solution. By Nullstellensatz, if $I=(x^3+y^3, y^3+xy)$, and $g(x,y)$ is satisfied $g(a,b)=0$ for all $(a,b)\in V(I)$, then $g(x,y)\in\sqrt{I}$ so there exists a natural number m such that $g^m\in I$.

Thus, we compute $V(I)$.

If $x^3+y^2=0$ and $y^3+xy=0$ simultaneously, then $x^3y+y^3-y^3-xy=0$ so $x^3y-xy=0$ so $xy(x^2-1)=0$. Thus, we have $x=0,1,-1$ or $y=0$. This gives the following points $(0,0),(1,i),(1,-i),(-1,1),(-1,-1)\in V(x^3+y^2,y^3+xy)$.

Since $(x+y)(x^2+y^4-2)$ $(0,0),(-1,1)$ immediately satisfy $(x+y)$, we need only check (x^2+y^4-2).

Since $1^2+(i)^4-2=1+1-2=0$, $1^2+(-i)^4-2=0$, $(-1)^2+(-1)^4-2=2-2=0$, we have by Nullstellensatz that $(x+y)(x^2+y^4-2)$ is satisfied by every point $(a,b)\in V(x^3+y^2,y^3+xy)$, so $(x+y)(x^2+y^4-2)\in\sqrt{I}$ and there exists an integer m such that $((x+y)(x^2+y^4-2))^m\in(x^3+y^2,y^3+xy)$. ✌

Problem 4. For integers $n, m > 1$, let $A \subset M_n(\mathbb{Z}_m)$ be a subring with the property that if $x \in A$ with $x^2 = 0$ then $x = 0$. Show that A is commutative. Is the converse true?

Solution. First, if $x^2 = 0 \implies x = 0$, then we note that if $x^n = 0 \implies x = 0$ for all n.

To see this, we simply note that for any positive integer n, there exists natural numbers s and $r < 2^s$ such that $n = 2^s + r$. Thus,

$$x^n = 0 \implies x^{2^s+r}x^{2^s-r} = x^{2^{s+1}} = (x^{2^s})^2 = 0.$$

Therefore, $x^{2^s} = (x^{2^{s-1}})^2 = 0$ and so on recursively until we obtain that $x = 0$.

Namely, A is a finite ring with no nilpotent elements.

Let $x \in J(A)$. Then because $J(A)$ is right quasi-regular, $1 - x$ is a unit in A.

Then, we construct a decreasing chain of ideals

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

which must terminate for some n. Namely, $(x^n) = (x^{n+1})$ so $x^n = rx^{n+1}$ for some $r \in A$. However, $rx \in J(A)$ and so $1 - rx$ is a unit. Therefore,

$$x^n = rx^{n+1} \implies x^n(1 - rx) = 0 \implies x^n = 0.$$

Namely, x is nilpotent. Since R has no nilpotent elements, $J(A) = 0$.

Thus, by Artin Wedderburn,

$$A \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_k}(D_k)$$

where the D_k are division rings.

Now, A contains no nilpotent elements, however matrix rings contain nilpotent elements over any division ring, since

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

is nilpotent of degree 2 over any division ring where $1 \neq 0$.

Namely, $n_i = 1$ for all i.

Finally, because the D_i are finite, by Wedderburn, the D_i are all fields.

Thus, A is a finite direct sum (isomorphic to a finite direct product) of fields and is therefore commutative.

Let

$$A = \left\{ \begin{bmatrix} a & 0 & 0 & \cdots & 0 & \mathbb{Z}_m \\ 0 & a & 0 & \cdots & 0 & 0 \\ 0 & 0 & a & \cdots & 0 & 0 \\ & \vdots & & \ddots & \vdots & \\ 0 & 0 & 0 & \cdots & a & 0 \\ 0 & 0 & 0 & \cdots & 0 & a \end{bmatrix} \mid a \in \mathbb{Z}_m \right\}$$

Then A is indeed a subring, it is commutative since every element of A is of the form $aX + bI$ where

$$X = \begin{bmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 0 & 0 \\ & \vdots & \ddots & \vdots & \\ 0 & 0 & \cdots & 0 & 0 \end{bmatrix} \qquad I = I_{n\times n}.$$

However, $X^2 = 0$ and $X \neq 0$. ✌

Problem 5. Let F be the splitting field of $f(x) = x^6 - 2$ over $\mathbb{Q}$. Show that $\text{Gal}(F/\mathbb{Q})$ is isomorphic to the dihedral group of order 12.

Solution. First, f is irreducible by Eisenstein with $p = 2$. 2 divides every coefficient of f except the leading coefficient and 2^2 does not divide the constant term.

Therefore, since f is irreducible over $\mathbb{Q}$, it is separable. Thus, F is the splitting field of a separable polynomial over $\mathbb{Q}$ and so $F/\mathbb{Q}$ is a Galois extension.

Next, let ξ be a 6^{th} root of unity. Then $\varphi(6) = \varphi(2)\varphi(3) = 1 \cdot 2 = 2$ so there are 2 primitive roots of unity.

Namely, $F = \mathbb{Q}(\xi, \sqrt[6]{2})$ and since $\xi \notin \mathbb{Q}(\sqrt[6]{2})$ because ξ is a complex number and $\mathbb{Q}(\sqrt[6]{2}) \subset \mathbb{R}$, we have that

$$[\mathbb{Q}(\xi, \sqrt[6]{2}) : \mathbb{Q}(\sqrt[6]{2})] = [\mathbb{Q}(\xi) : \mathbb{Q}] = 2.$$

Therefore,

$$[F : \mathbb{Q}] = [F : \mathbb{Q}(\sqrt[6]{2})][\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = 2 \cdot 6 = 12$$

Let $G = \text{Gal}(F/\mathbb{Q})$, then $|G| = 12$.

Now, let $\sigma \in G$ be defined by $\sigma(\sqrt[6]{2}) = \sqrt[6]{2}\xi$, $\sigma(\xi) = \xi$, and $\tau \in G$ be defined by $\tau(\sqrt[6]{2}\xi) = \sqrt[6]{2}\xi^{-1} =$.

Then, σ has order 6 since ξ is a primitive 6^{th} root of unity, and τ has order 2.

Now, note that $\sigma(\sqrt[6]{2}\xi^{j-1}) = \sqrt[6]{2}\xi^j$ so $\sigma^{-1}(\sqrt[6]{2}\xi^j) = \sqrt[6]{2}\xi^{j-1}$

Finally,

$$\sigma\tau(\sqrt[6]{2}\xi^j) = \sigma(\sqrt[6]{2}\xi^{-j}) = \sqrt[6]{2}\xi^{-j+1}$$

and

$$\tau\sigma^{-1}(\sqrt[6]{2}\xi^j) = \tau(\sqrt[6]{2}\xi^{j-1}) = \sqrt[6]{2}\xi^{-j+1}.$$

Therefore, G is described by

$$G \cong \langle \tau, \sigma \,|\, \tau^2 = \sigma^6 = 1, \sigma\tau = \tau\sigma^{-1} \rangle \cong D_{12}.$$

✌

Problem 6. Given that all groups of order 12 are solvable show that any group of order $2^2 \cdot 3 \cdot 7^2$ is solvable.

Solution. Let G be a group of order $2^2 \cdot 3 \cdot 7^2$. By Sylow, $n_7 \equiv 1 \mod 7$ and $n_7 | 12$. Thus, $n_7 = 1$ so G has a normal Sylow 7 subgroup.

Let P_7 be the Sylow 7-subgroup of G. Then $|P_7| = 7^2$, and so P_7 is abelian and namely solvable. Note that groups of order p^2 Q are abelian since they have nontrivial centers, and the quotient of their centers $Q/Z(Q)$ is cyclic so Q must be abelian.

Therefore, G has a normal subgroup which is solvable.

Finally, G/P_7 has order 12, which we are given implies that G/P_7 is a solvable group.

Therefore, G has a normal subgroup P_7 which is solvable and G/P_7 is solvable, so G itself is solvable. ✌