Kayla Orlinsky

Algebra Exam Spring 2015

Problem 1. Use Sylow's theorems and other results to describe, up to isomorphism, the possible structures of a group of order 1005.

Solution. Let G be a group of order $1005 = 3 \cdot 5 \cdot 67$. By Sylow, $n_{67} | 15$ and $n_{67} \equiv 1 \mod 67$ so clearly $n_{67} = 1$.

Now, we examine the cases.

$\boxed{\text{Abelian}}$ Then $G \cong \mathbb{Z}_{1005}$.

Let P_{67}, P_5, P_3 be Sylow $67, 5, 3$-subgroups respectively. Now, by the recognizing semi-direct products theorem. Since P_{67} is normal, P_3P_{67} and P_5P_{67} are subgroups of G, and since

$$|P_3P_5P_{67}| = 3 \cdot 5 \cdot 67/|P_3 \cap (P_5P_{67})| = 1005 = |G|$$

we have that G is a semi-direct product of its Sylow subgroups.

Since P_5P_{67} is a subgroup and has index 3 which is the smallest prime dividing the order of the group (see **Spring 2010: Problem 2 Claim 1**).

Therefore, P_5P_{67} is normal in G. Now, since P_5 is also a Sylow p-subgroup of P_5P_{67} and $n_5 = 1$ in P_5P_{67} by Sylow. Therefore, by **Fall 2011: Problem 5 Claim 3**, P_5 is also normal in G.

Finally, we have that P_3P_5 is a subgroup of G and so to determine possible structures of G as a semi-direct product, we need only look at three homomorphisms.

$\boxed{\varphi : P_3P_5 \to \text{Aut}(P_{67})}$ Since P_3P_5 is of order pq where $p \nmid (q-1)$, we have that $P_3P_5 \cong \mathbb{Z}_{15}$.

Furthermore, $\text{Aut}(P_{67}) \cong \mathbb{Z}_{66}$.

Thus, if $P_3 \cong \langle a \rangle$, $P_5 \cong \langle b \rangle$, and $P_{67} \cong \langle c \rangle$, we have that $\varphi(b) = \text{Id}$ since 5 does not divide the order of $\mathbb{Z}_{66}$ and $\varphi(a) = \alpha$ where α has order 3.

Since $\mathbb{Z}_{66}$ is abelian and $66 = 2 \cdot 3 \cdot 11$, there are exactly two non-trivial options for α. Note that one will be the square of the other. Namely, if $\varphi_1(a) = \alpha$ and $\varphi_2(a) = \alpha^2$, then $\varphi_1(a^2) = \varphi_2(a)$ and since $a \mapsto a^2$ is an automorphism of $\mathbb{Z}_3$, these will generate isomorphic semi-direct products.

Thus, we need only find one element of order 3 in $\mathbb{Z}_{66}$.

This element is given by $\alpha : \mathbb{Z}_{67} \to \mathbb{Z}_{67}$ defined by $\alpha(c) = c^{29}$.

Once can check that

$$\alpha^3(c) = \alpha^2(c^{29}) = \alpha(c^{37}) = c.$$

Therefore, we obtain a possible multiplication for G given by $bcb^{-1} = \varphi(b)(c) = c$ and $aca^{-1} = \varphi(a)(c) = c^{29}$.

Thus,

$$G \cong \langle a, b, c \,|\, a^3 = b^5 = c^{67} = 1, ab = ba, bc = cb, ac = c^{29}a \rangle.$$

$\boxed{\varphi : P_3P_{67} \to \mathrm{Aut}(P_5)}$ Since P_5 is normal, we can check $\varphi : P_3P_{67} \to P_5$, however $\mathrm{Aut}(P_5) \cong \mathbb{Z}_4$ and P_3P_{67} have no elements of order 2 or 4, so only the trivial homomorphism is possible.

$\boxed{\varphi : P_3 \to \mathrm{Aut}(P_5P_{67})}$ since 5 and 67 are coprime, $\mathrm{Aut}(P_5P_{67}) \cong \mathbb{Z}_4 \times \mathbb{Z}_{66}$. However, since there are no elements in $\mathbb{Z}_4$ of order 3, the only possible non-trivial homomorphisms will generate the same multiplication as the first case.

Therefore, there are only two groups of order 1005.

$$\mathbb{Z}_{1005}$$

$$\langle a, b, c \,|\, a^3 = b^5 = c^{67} = 1, ab = ba, bc = cb, ac = c^{29}a \rangle \cong \mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_{67} \times \mathbb{Z}_5$$

✌

Problem 2. Let R be a commutative ring with 1. Let M, N and V be R-modules.

(a) Show that if M and N are projective, then so is $M \otimes_R N$.

(b) Let $\operatorname{tr}(V) = \{\sum_i \varphi_i(v_i) \mid \varphi \in \operatorname{Hom}_R(V, R), v_i \in V\} \subset R$. If $1 \in \operatorname{tr}(V)$, show that up to isomorphism, R is a direct summand of V^k for some k.

Solution.

(a) Since M and N are projective, there exists A, B, R-modules such that

$$M \oplus A \cong R^m \qquad N \oplus B \cong R^n$$

where $R^m \cong \bigoplus_{i=1}^m R_i$ and R^n are free modules of dimension m and n respectively.

Thus,

$$\begin{aligned}
(M \otimes_R N) \oplus [(A \otimes_R N) \oplus B^m] &= [(M \oplus A) \otimes_R N] \oplus B^m \\
&= [R^m \otimes_R N] \oplus B^m \\
&= [(R \oplus R \oplus \cdots \oplus R) \otimes_R N] \oplus B^m \\
&= [N \oplus N \oplus \cdots \oplus N] \oplus B^m \qquad (1) \\
&= (N \oplus B) \oplus (N \oplus B) \oplus \cdots \oplus (N \oplus B) \\
&= R^n \oplus R^n \oplus \cdots \oplus R^n \\
&= R^{nm}
\end{aligned}$$

with (1) because $R \otimes_R N = N$. Therefore, $M \otimes_R N$ is the summand of a free module so it is projective.

(b) Let

$$\operatorname{tr}(V) = \{\sum_i \varphi_i(v_i) \mid \varphi \in \operatorname{Hom}_R(V, R), v_i \in V\} \subset R.$$

Now, we note that $\operatorname{tr}(V) = \sum \varphi(V)$ where the sum is taken over all $\varphi \in \hom_R(V, R)$. Furthermore, because φ is homomorphism, it is easily verified that $\varphi(V)$ is an ideal of R for all φ.

Now, $\operatorname{tr}(V)$ is an ideal of R since it is clearly closed under addition and for any $r \in R$,

$$r \sum_i \varphi_i(v_i) = \sum_i \varphi_i(rv_i) \in \operatorname{tr}(V)$$

since the φ are homomorphisms and $rv_i \in V$ since V is an R-modules. This gives that $\operatorname{tr}(V)$ is a left ideal and since R is commutative it will be a right ideal as well.

Therefore, if $1 \in \operatorname{tr}(V)$ then $\operatorname{tr}(V) = R$. Thus, there exists finitely many $\varphi_i \in \operatorname{Hom}_R(V, R)$ and $v_i \in V$ such that

$$1 = \varphi_1(v_1) + \cdots + \varphi_k(v_k) \qquad k \text{ minimal.}$$

Namely, for every $r \in R$, there exists $w_j \in V$ such that

$$r = \varphi_1(w_1) + \cdots + \varphi_k(w_k).$$

Now, because k is minimal, if

$$r \in \varphi_i(V) \cap \bigoplus_{j \neq i} \varphi_j(V)$$

then

$$r = \varphi_i(w_i) = \sum_{j \neq i} \varphi_j(w_j)$$

Thus, we can define

$$\begin{gathered} f : V^k \to R \\ (w_1, ..., w_k) \mapsto \sum_{i=1}^{k} \varphi_i(w_i) \end{gathered}$$

which we have already found to be surjective.

Therefore, we have a short exact sequence

$$0 \longrightarrow \ker(f) \longrightarrow V^k \longrightarrow R \longrightarrow 0$$

However, R is a free module over itself, so R is projective. Therefore, the above short exact sequence is split and so by the splitting lemma,

$$V^k \cong R \oplus \ker(f).$$

Therefore, R is a direct summand of V^k.

✌

Problem 3. Let F be a field and M a maximal ideal of $F[x_1, ..., x_n]$. Let K be an algebraic closure of F. Show that M is contained in at least 1 and in only finitely many maximal ideals of $K[x_1, ..., x_n]$.

Solution. First, by generalized Nullstellensatz, $V(M) \neq \varnothing$ as a subset of K^n, since M is maximal in $F[x_1, ..., x_n]$ so $1 \notin M$.

Namely, there exists $(a_1, ..., a_n) \in K^n$ such that $(a_1, ..., a_n) \in V(M)$.

Therefore, again by Nullstellensatz, for every $f \in M$, there exists m such that $f^m \in (x_1 - a_1, ..., x_n - a_n)$ which is a maximal ideal of $K[x_1, ..., x_n]$.

However, maximal ideals are prime, and so inductively, we get that $f \in (x_1 - a_1, ..., x_n - a_n)$. Therefore, $M \subset (x_1 - a_1, ..., x_n - a_n)$ so M is contained in at least one maximal ideal.

Next, we prove a claim about $L = F[x_1, ..., x_n]/M$.

Claim 1. If $L = F[x_1, ..., x_n]/M$ is a field, then it 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

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

✌

Now, if N is a maximal ideal of $K[x_1, ..., x_n]$ such that $M \subset N$, then we will clearly have an embedding

$$L \hookrightarrow K[x_1, ..., x_n]/N \cong K$$

induced by the embedding $M \hookrightarrow N$. Note that since $K[x_1, ..., x_n]/N$ is a finite field extension of K which is algebraically closed, it must be isomorphic to K.

Namely, each embedding of L is associated to exactly one maximal ideal N of $K[x_1, ..., x_n]$ such that $M \subset N$.

Claim 2. If L is a finite field extension of F, then there exists only finitely many embeddings of L into K the algebraic closure of F.

Proof. We proceed by induction.

Basecase: let $L = F(a_1)$. Because a_1 is algebraic over F, it has minimal (irreducible) polynomial

$$f(x) = x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_1 x + \alpha_0 \in F[x].$$

Now, if $\varphi : L \hookrightarrow K$, because $\varphi(1) = 1$, φ is F-linear and so

$$\varphi(f(a_1)) = \varphi(a_1)^n + \alpha_{n-1}\varphi(a_1)^{n-1} + \cdots + \alpha_1\varphi(a_1) + \alpha_0 = 0$$

so φ permutes the roots of $f(x)$. Note that K is the algebraic closure of F and so contains all such roots.

Thus, there are only finitely many possible choices of φ since there are only finitely many roots of $f(x)$.

Now, assume there are only finitely many injections of $L = F(a_1, ..., a_k)$ to K for $k \leq n$.

Then we examine $L = F(a_1, ..., a_n, a_{n+1}) = F(a_1, ..., a_n)(a_{n+1})$. Then there are only finitely many $F(a_1, ..., a_n)$-linear injections from $L \hookrightarrow K$ by the same reasoning as the basecase, and by the induction hypothesis, only finitely many F-linear injections from $F(a_1, ..., a_n) \hookrightarrow K$.

Since any injection $L \hookrightarrow K$ will be defined by where it sends the a_i, and since there are only finitely many choices for where to send $a_1, ..., a_n$ and only finitely many choices for where to send a_{n+1}, we have only finitely many possible injections of L into K. ✌

Finally, since there are only finitely many possible embeddings of $F[x_1, ..., x_n]/M$ to $K[x_1, ..., x_n]/N$ there can be only finitely many maximal ideals $M \subset N$. ✌

Problem 4. Let F be a finite field.

(a) Show that there are irreducible polynomials over F of every positive degree.

(b) Show that x^4+1 is irreducible over $\mathbb{Q}[x]$ but is reducible over $\mathbb{F}_p[x]$ for every prime p (hint: show there is a root in $\mathbb{F}_{p^2}[x]$).

Solution.

(a) Let F be a finite field of $q = p^k$ elements. Fix a positive integer n.

Then let K be the field of $q^n = p^{nk}$ elements. Then $K^\times$ is a cyclic multiplicative group. Now, because finite fields of the same order are isomoprhic, K is isomorphic to a field extension of F.

Therefore,

$$[K : F] = \frac{[K : F_p]}{[F : F_p]} = \frac{nk}{k} = n$$

where F_p is the field of p elements. Thus, there exists an element $\alpha \in K$ such that α has minimal polynomial of degree n over F.

By definition, the minimal polynomial is irreducible and has degree n over F.

(b) First, x^4+1 has no roots in $\mathbb{Q}$ so if it reduces it has no linear terms. Namely, it can only reduce into a product of two quadratic polynomials. However, $x^4+1 = (x^2-i)(x^2+i)$ over $\mathbb{C}[x]$ and since $i \notin \mathbb{Q}$, we have that x^4+1 is irreducible.

Now, we examine x^4+1 as a polynomial over $\mathbb{F}_p[x]$.

If $p = 2$, then

$$x^4+1 = (x^2)^2 + 1^2 = (x^2+1)^2$$

and so it is reducible.

If p is odd, then $p = 2k+1$ and $k \geq 1$.

$$p^2 = (2k+1)^2 = 4k^2+4k+1 = 4(k^2+k)+1 = 8r+1$$

since if k is even, k^2+k is also even, and if k is odd, then k^2+k is a sum of two odds and so it is also even.

Namely, $p^2 \equiv 1 \mod 8$ for any odd p. Therefore,

$$(x^8-1)|(x^{p^2-1}-1).$$

However, then if α is a root of x^4+1, then α is a root of $(x^4+1)(x^4-1) = x^8-1$ and so it is a root of $x^{p^2-1}-1$. Finally, we have that

$$\alpha^{p^2-1} = 1 \implies \alpha^{p^2} = \alpha$$

and so $\alpha \in \mathbb{F}_{p^2}$.

Now, if x^4+1 is irreducible over $\mathbb{F}_p[x]$ and α is a root of x^4+1, then $[\mathbb{F}_p(\alpha):\mathbb{F}_p]=4$.

However, $\alpha \in \mathbb{F}_{p^2}$ and so

$$2=[\mathbb{F}_{p^2}:\mathbb{F}_p]=[\mathbb{F}_{p^2}:\mathbb{F}_p(\alpha)][\mathbb{F}_p(\alpha):\mathbb{F}_p]=[\mathbb{F}_{p^2}:\mathbb{F}_p(\alpha)]4$$

which is clearly a contradiction.

Thus, x^4+1 is reducible over $\mathbb{F}_p$.

✌

Problem 5. Let F be a field and M a finitely generated $F[x]$-module. Show that M is artinian if and only if $\dim_F M$ is finite.

Solution.

$\boxed{\implies}$ Assume M is artinian. Because M is finitely generated,

$$M = F[x]m_1 + \cdots + F[x]m_n$$

for some $m_i \in M$.

We proceed by induction on n.

Assume $M = F[x]m_1$ for some $m_1 \in M$.

Then let

$$\begin{aligned} \varphi : F[x] &\to M \\ f(x) &\mapsto f(x)m_1 \end{aligned}$$

The $\ker(\varphi) = \mathrm{Ann}(m_1)$ by definition. Therefore,

$$F[x]/\mathrm{Ann}(m_1) \cong M$$

which is Artinian. Namely, $F[x]/\mathrm{Ann}(m_1)$ must be a field extension of F since the only artinian domains are fields.

> **Claim 3.** An artinian integral domain F is a field.
>
> *Proof.* Let $a \in F$ be nonzero. Then we have a decreasing chain of ideals
>
> $$(a) \supset (a^2) \supset (a^3) \supset \cdots$$
>
> which must terminate after a finite number of steps. Thus, $(a^l) = (a^k)$ for all $l \geq k$ for some k.
>
> Namely, $a^{k+1}b = a^k$ for some $b \in F$.
>
> However, then $a^k(ab - 1) = 0$ and since F is a domain, $a \neq 0$ implies that $a^k \neq 0$ and so $ab = 1$. Thus, a has a right inverse.
>
> Similarly, a has a left inverse so a is invertible. Therefore, F is a field. ✌

Now, since $F[x]/\mathrm{Ann}(m_1)$ is a field extension of F, and since $F[x]$ is a PID, $\mathrm{Ann}(m_1)$ must be generated by an irreducble polynomial. Therefore, $[F[x]/\mathrm{Ann}(m_1) : F] < \infty$ since it is an algebraic extension of F, and so $M \cong F[x]/\mathrm{Ann}(m_1)$ is a finite dimensional F-vector space.

Now, assume

$$M = F[x]m_1 + \cdots + F[x]m_k$$

is a finite dimensional F-vector space for all $k \leq n$.

Then assume

$$M = F[x]m_1 + \cdots + F[x]m_n + F[x]m_{n+1}.$$

Then $N = F[x]m_1 + \cdots + F[x]m_n$ is a submodule of M which a finite dimensional F-vector space by the inductive hypothesis.

Thus, $M/N \cong F[x]m_{n+1}$ is an artinian $F[x]$-module and so it is finite dimensional F-vector space by the same reasoning as the basecase. Thus, M/N and N are both finite dimensional over F and so M must be finite dimensional over F.

$\boxed{\Longleftarrow}$ Because M is finitely generated as an $F[x]$-module

$$M = F[x]m_1 + \cdots + F[x]m_n$$

for some $m_i \in M$. However, because M is a finite dimensional vector space over F, $M = x_1F + \cdots + x_mF$ for $x_1, ..., x_m \in M$ linearly independent. Thus, $f(x)m_i$ can be written as a unique linear combination of the x_i, and so any $F[x]$-submodule of M will be an F-subspace of M.

Therefore, any decreasing chain of submodules of M is a decreasing chain of finite dimensional subspaces which must terminate after a finite number of steps. Thus, M is artiniain as an $F[x]$-module.

✌

Problem 6. Let R be a right Artinian ring with a faithful irreducible right R-module. If $x, y \in R$, set $[x, y] := xy - yx$. Show that if $[[x, y], z] = 0$ for all $x, y, z \in R$, then R has no nilpotent elements.

Solution. A faithful right R-module is a right R-module where $\text{Ann}(M) = 0$.

An irreducible R-module is equivalent to a simple R-module.

Since $J(R)$ is also defined as the intersection of the annihilators of all simple right R-modules, $J(R) = 0$ since R has a simple right-module with trivial annihilator.

Therefore, by Artin-Wedderburn, R is semi-simple and so

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

as a right R-module where D_k are division rings over R.

Let $n_i > 1$ for some i. Then we define the following matrices:

Let

$$x = \begin{bmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 0 & 0 \\ & \vdots & \ddots & \vdots & \\ 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 \end{bmatrix} \qquad y = \begin{bmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 1 & 0 \\ & \vdots & \ddots & \vdots & \\ 0 & 1 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \end{bmatrix} \qquad z = x$$

Then

$$x^2 = 0$$

and

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

Therefore,

$$\begin{aligned} [[x, y], x] &= [(xy - yx), x] \\ &= (xy - yx)x - x(xy - yx) \\ &= xyx - yx^2 - x^2y + xyx \\ &= 2xyx \\ &= 2x \\ &= 0 \end{aligned}$$

however, $2x \neq 0$ and this contradicts the assumption that $[[x, y], z] = 0$ for all $x, y, z \in R$ and so $n_i = 1$ for all i.

Namely, R is a direct sum of division rings and so has no nilpotent elements. ✌