Kayla Orlinsky

Algebra Exam Spring 2017

Problem 1. Let R be a PID. Let M be an R-module.

(a) Show that if M is finitely generated, then M is cyclic if and only if M/PM is for all prime ideals P of R.

(b) Show that the previous statement is false if M is not finitely generated.

***Note as written this problem is wrong unless we assume P is a *nonzero* prime ideal.

Solution.

(a) This is very similar to **Fall 2013: Problem 2**.

Let M be finitely generated.

$\boxed{\Longrightarrow}$ Assume M is cyclic. Then $M = (x) = xR = \{rx \,|\, r \in R\}$ for some $x \in X$. However, then M/PM is certainly cyclic since any quotient of a cyclic module must also be cyclic.

This is because we can define $\pi : M \to M/PM$ to be the quotient map, which is surjective. Then $M/PM \cong \pi((x)) = (\pi(x))$ and so is cyclic.

$\boxed{\Longleftarrow}$ Assume M/PM is cyclic for all *nonzero* prime ideals P.

By the structure theorem, there is a chain of ideals

$$(d_1) \subset (d_2) \subset \cdots \subset (d_n)$$

such that

$$M \cong R/(d_1) \oplus \cdots \oplus R/(d_n).$$

Note that $d_i | d_{i-1}$ for all i.

If (d_n) is not maximal, then there is a maximal (prime) ideal P such that $(d_n) \subset P$.

Then $PM = P/(d_1) \oplus \cdots \oplus P/(d_n)$ so Then

$$M/PM \cong (R/(d_1))/(P/(d_1)) \oplus \cdots \oplus (R/(d_n))/(P/(d_n)) \cong (R/P)^n$$

However, M/PM is cyclic for all P, and $(R/P)^n \cong R/(a)$ for some a forces $n = 1$. Namely, M is cyclic.

(b) As written, the problem is true regardless of whether or not M is finitely generated. Since R is a PID, it is a domain, so $P = (0)$ is a prime ideal. However, then $PM = (0)M = 0$ so $M/PM \cong M$ is cyclic.

However, with the assumption that we may use only *nonzero* prime ideals, let $R = \mathbb{Z}$ which is a PID and $M = \mathbb{Q}$. Then M is infinitely generated.

The *nonzero* prime ideals of R are exactly ideals generated by (p) where p is a prime and $(p)M = M$.

Therefore,

$$M/(p)M \cong M/M \cong (0)$$

which is certainly cyclic.

However, M is not cyclic.

✌

Problem 2. Prove that a power of the polynomial $(x+y)(x^2+y^4-2)$ belongs to the ideal (x^3+y^2, x^3+xy) in $\mathbb{C}[x,y]$.

Solution. It suffices to show that $(x+y)(x^2+y^4-2)$ is satisfied by all zeros in $V(x^3+y^2, x^3+xy)$.

By Nullstellenzatz, if $g(x,y)$ is a polynomial such that $g(a,b)=0$ for all $(a,b) \in V(I)$, then there exists an n such that $g^n(x,y) \in I$.

Let $g(x,y) = (x+y)(x^2+y^4-2)$

Now, we examine $V(x^3+y^2, x^3+xy)$.

Clearly $(0,0) \in V(x^3+y^2, x^3+xy)$. If $x^3+y^2=0$ and $x^3+xy=0$ then $y^2-xy=0$, so $y(y-x)=0$.

If $y=0$ then $x=0$, and if $y=x$, then $x^2(x+1)=0$, so $x=-1$.

Thus, the only elements of $V(x^3+y^2, x^3+xy)$ are $(0,0), (-1,-1)$.

Since $g(0,0)=0$ and $g(-1,-1)=0$, we have that there exists an n such that $g^n(x,y) \in (x^3+y^2, x^3+xy)$. ✌

Problem 3. Let G be a finite group with a cyclic Sylow 2-subgroup S.

(a) Show that $N_G(S) = C_G(S)$.

(b) Show that if $S \neq 1$, then G contains a normal subgroup of index 2. (hint: suppose that $n = [G : S]$, consider an appropriate homomorphism from $G \to S_n$).

(c) Show that G has a normal subgroup N of odd order such that $G = NS$.

Solution. This problem is very similar to **Spring 2011: Problem 1.**

(a) We will prove the stronger version of this problem using **Spring 2011: Problem 1, (a)**.

> **Claim 1.** If p is the smallest prime dividing $|G|$ and P is a cyclic Sylow p-subgroup, then $N_G(P) = C_G(P)$.
>
> *Proof.* Let p be the smallest prime dividng $|G|$. Then, since
>
> $$P \trianglelefteq C_G(P) \trianglelefteq N_G(P)$$
>
> we have that
>
> $$[N_G(P) : C_G(P)] = n \qquad \gcd(n, p) = 1.$$
>
> Furthermore, because p is the smallest prime dividing $|G|$, n is only divisible by primes q with $q > p$.
>
> Now, let
>
> $$\begin{aligned} \varphi : N_G(P) &\to \mathrm{Aut}(P) \\ a &\mapsto \sigma_a \end{aligned}$$
>
> be the map of the conjugation action of $N_G(P)$ on P.
>
> Then $C_G(P)$ is clearly the kernel of this action and so by the first isomorphism theorem,
>
> $$N_G(P)/C_G(P) \cong A \subset \mathrm{Aut}(P).$$
>
> Finally, because $P = \langle x \rangle$ is cyclic, we have that the automorphisms of P are exactly the maps $x \mapsto x^k$ for $\gcd(k, p) = 1$. Namely,
>
> $$|\mathrm{Aut}(P)| = p^{l-1}(p-1) \qquad \text{by the Euler Totient Function}$$

> assuming that $|P| = p^l$. Since the divisors of this are not greater than p, and $|N_G(P)/C_G(P)|$ has only divisors greater than p, it must be that $|N_G(P)/C_G(P)| = 1$.
>
> Namely,
> $$N_G(P) = C_G(P).$$

✌

(b) Assume $S \neq 1$. Then let $n = |G|/|S|$. Note that n is odd. Let

$$\varphi : G \to S_{|G|}$$
$$a \mapsto \tau_a$$

where $\tau_a(g) = ag$ is the left multiplication map.

Then φ is certainly injective since $\tau_a = \mathrm{Id}$ if and only if $a = e$.

Now, if $S = \langle a \rangle$, then $\varphi(a) = \tau_a$ is a cycle of order $|S|$ which is even. Now, let $g \in G$, then $\tau_a(g) = ag$ and $\tau_a(ag) = a^2 g$ so $\varphi(a)$ has a cycle of the form $(g, ag, a^2g, ..., a^{|S|-1}g)$. Since
$$\tau_a(a^k) = a^{k+1} = \tau_{a^{k+1}}(e) = (\tau_a)^{k+1}(e),$$
we see that
$$\varphi(a) = (a, a^2, ..., a^{|S|-1}) \prod_{g \in G \setminus S} (g, ag, a^2g, ..., a^{|S|-1}g).$$

Namely, $\varphi(a)$ is a product of n cycles of even length, so $\varphi(a)$ is an odd permutation.

Finally, let
$$\mathrm{sgn} : S_{|G|} \to \{1, -1\}$$
be the sign map. Then since $\mathrm{sgn}(\mathrm{Id}) = 1$, and $\mathrm{sgn}(\varphi(a)) = -1$, we have that

$$\mathrm{sgn} \circ \varphi : G \to \{1, -1\}$$

is surjective.

Therefore, $G/\ker(\mathrm{sgn} \circ \varphi) \cong \mathbb{Z}_2$ so G has a normal (because it is a kernel) subgroup, $H = \ker(\mathrm{sgn} \circ \varphi)$ of index 2.

(c) Let $|G| = 2^r n$. Then we proceed by induction on r.

For $r = 1$, we are done since by (b), G has a normal subgroup H of index 2. Namely, $|H| = n$. Therefore,

$$|SH| = |S||H|/|S \cap H| = |S||H|/1 = 2n = |G|$$

and since H is normal, SH is a subgroup of G so $SH = G$.

Now, assume the statement holds for all $1 \leq k \leq r$. Then let $|G| = 2^{r+1}n$ and have a cylic Sylow 2-subgroup S.

From (b), G has a normal subgroup H of order $2^r n$. Now, $S \cap H$ will also be cyclic subgroup. Now, H is normal so SH is a subgroup of G. Since $S \not\subset H$, it must be that $|SH| > H$ so $SH = G$.

Finally
$$|S \cap H| = |S||H|/|SH| = 2^{r+1}2^r n/2^{r+1}n = 2^r$$
so H has a cyclic Sylow 2-subgroup $S \cap H$.

Therefore, by the inductive hypothesis, there exists an N normal subgroup of H of order n such that $H = (S \cap H)N$. Now, N is also a subgroup of G so it suffices to show that N is normal.

However, clearly any element $g \in G$ normalizes n. Since N is exactly all the elements in G of odd order. Therefore, gng^{-1} has odd order and so it is in N.

Thus, N is normal in G so
$$G = SN.$$

✌

Problem 4. Show that $\mathbb{Z}[\sqrt{5}]$ is not integrally closed in its quotient field.

Solution. First, we note that if $a + b\sqrt{5} \in \mathbb{Q}[\sqrt{5}]$, then $a + b\sqrt{5}$ satisfies

$$(x - a - b\sqrt{5})(x - a + b\sqrt{5}) = x^2 - 2ax + a^2 - 5b^2 \in \mathbb{Q}[x].$$

And this polynomial is minimal over $\mathbb{Q}[x]$, since $a + b\sqrt{5} \notin \mathbb{Q}$.

Now, clearly $\frac{1+\sqrt{5}}{2}$ is in the field of fractions of $\mathbb{Z}[\sqrt{5}]$. Furthermore, it has minimal polynomial

$$x^2 - \frac{2}{2}x + \frac{1}{4} - \frac{5}{4} = x^2 - x - 1 \in \mathbb{Z}[x].$$

Therefore, $\frac{1+\sqrt{5}}{2}$ is integral over $\mathbb{Z}$ and so it is integral over $\mathbb{Z}[\sqrt{5}]$. However, clearly $\frac{1+\sqrt{5}}{2} \notin \mathbb{Z}[\sqrt{5}]$ so $\mathbb{Z}[\sqrt{5}]$ is not integrally closed. ✌

Problem 5. Let $f(x) = x^{11} - 5 \in \mathbb{Q}[x]$.

(a) Show that f is irreducible in $\mathbb{Q}[x]$.

(b) Let K be the splitting field of f over $\mathbb{Q}$. What is the Galois group of $K/\mathbb{Q}$.

(c) How many subfields L of K are there such that $[K : L] = 11$.

Solution.

(a) We will apply Eisenstein's with $p = 5$. Then p does not divide the leading coefficient of f, p does divide every other coefficient, and p^2 does not divide the constant term.

Therefore, by Eisenstein's Criteion, $f(x)$ is irreducible over $\mathbb{Q}[x]$.

(b) Let K be the splitting field of f over $\mathbb{Q}$.

Let $z^{11} = 5$ and $z = re^{i\theta}$. Then $r = \sqrt[11]{5}$ and $11\theta = 2k\pi$ for $k = 1, ..., 11$. Clearly, $\sqrt[11]{5}\xi$ where $\xi = e^{2i\pi/11}$ is a primitive root of $f(x)$.

Therefore,
$$K = \mathbb{Q}(\sqrt[11]{5}, \xi).$$

Now, since ξ^{11} is primitive, it satisfies $g(x) = x^{10} + x^9 + \cdots + x + 1$.

Therefore,
$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt[11]{5})][\mathbb{Q}(\sqrt[11]{5}) : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt[11]{5})]11$$
and
$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\xi)][\mathbb{Q}(\xi) : \mathbb{Q}] = [K : \mathbb{Q}(\xi)]10.$$

Thus, 110 divides $[K : \mathbb{Q}]$ and since $[K : \mathbb{Q}] \leq 10$, we have that $[K : \mathbb{Q}] = 110$. Now, since K is the splitting field of a separable (no repeated roots) polynomial, $K/\mathbb{Q}$ is Galois so $G = \mathrm{Gal}(K/\mathbb{Q})$ exists and $|G| = 110 = 2 \cdot 5 \cdot 11$.

Now, let $\sigma : K \to K$ be an element of G. Then $\sigma(\sqrt[11]{5}) = \sqrt[11]{5}\xi^i$ and $\sigma(\xi) = \xi^j$ for some $i, j = 1, ..., 11$.

Note that if $\sigma(\sqrt[11]{5}) = \sqrt[11]{5}$ and $\sigma(\xi) = \xi^i$ and $\tau(\sqrt[11]{5}) = \sqrt[11]{5}\xi^j$ and $\tau(\xi) = \xi$, then
$$\sigma\tau(\sqrt[11]{5}\xi) = \sigma(\sqrt[11]{5}\xi^{j+1}) = \sqrt[11]{5}\xi^{(j+1)i}$$
and
$$\tau\sigma(\sqrt[11]{5}\xi) = \tau(\sqrt[11]{5}\xi^i) = \sqrt[11]{5}\xi^{j+i}$$

Namely, we obtain immediately that G is non-abelian.

Finally, if $\sigma : K \to K$ is defined by $\sigma(\sqrt[11]{5}) = \sqrt[11]{5}\xi$ and $\sigma(\xi) = \xi^2$, then one can check that σ has order 10.

Namely, G has a subgroup $H = \langle\sigma\rangle$ of order 10.

Now, if P_{11} is a Sylow 11-subgroups, and since n_{11} the number of Sylow 11-subgroups must divide $|G|/11 = 10$ by the Sylow theorems, $n_{11} = 1$. Note that $\rho : K \to K$ defined by $\rho(\sqrt[11]{5}) = \sqrt[11]{5}\xi^2$ and $\rho(\xi) = \xi$ has order 11. Thus, $P_{11} = \langle \rho \rangle$.

So $P_{11} \cong \mathbb{Z}_{11}$ is normal in G. Therefore, $P_{11}H$ is a subgroup of G and since $|P_{11}H| = |G|$, we have that G must be a semi-direct product of P_{11} and H.

Now, we must identify the multiplication on G. Since

$$G \cong \langle \rho \rangle \rtimes_{\varphi} \langle \sigma \rangle$$

where $\varphi : \langle \sigma \rangle \to \mathbb{Z}_{10}$ and multiplication on G is defined by $\varphi(\sigma)(\rho) = \sigma\rho\sigma^{-1} = \rho^t$ for some t such that $\rho \mapsto \rho^t$ is an automorphism of P_{11}.

Since $\sigma(\sqrt[11]{5}\xi^5) = \sqrt[11]{5}\xi\xi^{10} = \sqrt[11]{5}$, we have that $\sigma^{-1}(\sqrt[11]{5}) = \sqrt[11]{5}\xi^5$ and $\sigma(\xi^6) = \xi$ so

$$\begin{aligned}
\sigma\rho\sigma^{-1}(\sqrt[11]{5}) &= \sigma\rho(\sqrt[11]{5}\xi^5) \\
&= \sigma(\sqrt[11]{5}\xi^7) \\
&= \sqrt[11]{5}\xi^{15} \\
&= \sqrt[11]{5}\xi^4 \\
\sigma\rho\sigma^{-1}(\xi) &= \sigma\rho(\xi^6) \\
&= \sigma(\xi^6) \\
&= \xi
\end{aligned}$$

so $\sigma\rho\sigma^{-1} = \rho^2$.

Therefore,

$$G \cong \langle \sigma, \rho \,|\, \sigma^{10} = \rho^{11} = 1, \sigma\rho\sigma^{-1} = \rho^2 \rangle.$$

(c) The subfields L of K such that $[K : L] = 11$ correspond exactly to the subgroups H of G such that $|H| = 11$ (namely, so $[G : H] = |G|/11 = 10$).

Since if H is a subgroup of G of order 11, it is a Sylow 11-subgroup, and since n_{11} the number of Sylow 11-subgroups must divide $|G|/11 = 10$ by the Sylow theorems, $n_{11} = 1$.

Thus, G has exactly one Sylow 11 subgroup and it is normal.

Thus, K contains one subfield L such that $[K : L] = 11$ and in fact, $L/\mathbb{Q}$ is Galois.

✌

Problem 6. Suppose that R is a finite ring with 1 such that every unit of R has order dividing 24. Classify all such R.

Solution. Since R is finite, it is trivially artinian. Now, $R' = R/J(R)$ has trivial Jacobson and is also artinian. Thus, by Artin Wedderburn, $R' \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_k}(D_k)$ where D_i are division rings.

Since R is finite, each D_i is finite, and so each must be a finite field. Note that if $|D_i| = p_i^m$ then $|D_i^\times| = p_i^{m-1}(p_i - 1)$. Furthermore, $D_i^\times$ is the group of units of D_i and so since each unit of R' divides 24, we have that $p_i^{m-1}(p_i-1)|24$. Namely, we have the follwing options for pairs,

$$(p, m) = (2, 1), (2, 2), (2, 3), (2, 4), (3, 1), (3, 2), (5, 1), (7, 1), (13, 1).$$

Alternatively,

$$|D_i| = 2, 4, 8, 16, 3, 9, 5, 7, 13.$$

Now, units in $M_{n_i}(D_i)$ are exactly elements in $GL_{n_i}(D_i)$. Since

$$|GL_{n_i}(D_i)| = (|D_i|^{n_i} - 1)(|D_i|^{n_i} - |D_i|) \cdots (|D_i|^{n_i} - |D_i|^{n_i-1}),$$

we now have that $(|D_i|^{n_i} - 1)(|D_i|^{n_i} - |D_i|) \cdots (|D_i|^{n_i} - |D_i|^{n_i-1})$ must divide 24. If $n_i = 1$, then we simply hav a copy of D_i which we have already found.

Now, this gives the following possible pairs

$$(n_i, |D_i|) = (2, 2).$$

Everything else grows past 24.

Therefore, R' is a direct sum of copies of D_i, which can be any of the finite fields previously described and some number of copies of $M_2(\mathbb{Z}_2)$.

Finally, since $R/J(R)$ is finite, it is finitely generated as an R-module.

Write $R/J(R) = \overline{x_1}R + \cdots + \overline{x_n}R$ for some $\overline{x_i} = x_i + J(R) \in R/J(R)$.

Then, by Nakayama's Lemma, $R \cong x_1R + \cdots + x_nR$.

This fully describes R. ✌