Kayla Orlinsky

Algebra Exam Fall 2017

Problem 1. Assume S is a commutative integral domain, and $R \subset S$ is a subring. Assume S is finitely generated as an R-module, i.e., there exists elements $s_1, ..., s_n \in S$ such that $S = s_1R + s_2R + \cdots s_nR$. Show that R is a field if and only if S is a field. Is the statement true if the assumption that S is an integral domain is dropped?

Solution.

***Note that here, finitely generated as an R-module is far stronger than finitely generated as an R-algebra.
If S were a finitely generated R-algebra, then $S = R[s_1, ..., s_n]$, namely, S would consist of all polynomials in the s_i with coefficients in R.
To say that S is finitely generated as an R-module, is to say that every element of S is a finite sum of the s_i with coefficients in R.

$\boxed{\Longrightarrow}$ Assume R is a field. Since S is commutative and has no zero divisors, to show that S is a field, we need only show that every $s \in S^\times$ is a unit.

Fix $0 \neq s \in S$

$$\begin{aligned} \varphi : S &\to S \\ t &\mapsto st \end{aligned}$$

φ is clearly an R-module homomorphism since it is linear.

Furthermore, since S is a domain, φ is injective since if $\varphi(t) = 0$ then $st = 0$ so either $s = 0$ or $t = 0$, but $s \neq 0$ so $t = 0$.

However, since S is a finitely generated module over a field, S is an R-vector space. Therefore, since S is a finitely generated vector space, it has a finite basis and is finite dimensional.

Finally, this forces φ to also be surjective by rank-nullity theorem.

Thus, $1 \in R \subset S$ and so, there exists $t \in S$ so $\varphi(t) = st = 1$. Namely, s has an inverse in S.

Since $s \in S^\times$ was arbitrary, we have that S is a field.

$\boxed{\Longleftarrow}$ Assume S is a field. Since $s_i^k \in S$ for all k, (S is a ring), we have that $R[s_i] \subset S$. However, since S is finitely generated as an R-module, then $R[s_i]$ is also finitely generated as an R-module, and so namely, s_i is transcendental over R.

To see this, note that if $R[s_i]$ is spanned by $\{1, f_1(s_i), ..., f_l(s_i)\}$ where $f_j \in R[s_1, ..., s_n]$, then if m is the maximal degree of the f_j,

$$s_i^{m+1} = r_0 + \sum_{j=1}^{n} r_j f_j(s_i) \qquad r_j \in R$$

and so s_i satisfies a monic polynomial with coefficeints in R.

Therefore, S is an algebraic extension of R.

However, now we are done. Let $0 \neq r \in R$, then $r^{-1} \in S$ since S is a field.

However, r^{-1} is algebraic over R, meaning that there exists $a_i \in R$ not all 0 so

$$\begin{aligned}
(r^{-1})^m + a_{m-1}(r^{-1})^{m-1} + \cdots + a_1 r^{-1} + a_0 &= 0 \\
r^{m-1}((r^{-1})^m + a_{m-1}(r^{-1})^{m-1} + \cdots + a_1 r^{-1} + a_0) &= 0 \\
r^{-1} + a_{m-1} + a_{m-2}r + \cdots + a_1 r^{m-2} + a_0 r^{m-1} &= 0 \\
r^{-1} &= -a_0 r^{m-1} - a_1 r^{m-2} - \cdots - a_{m-2}r - a_{m-1} \in R
\end{aligned}$$

Therefore, R is a field.

The statement is false if the assumption that S is an integral domain is dropped.
$\boxed{\Longrightarrow}$ Let $R = \mathbb{Z}_3$, $S = R[\sqrt{3}]$. Then S is finitely generated as a $\mathbb{Z}_3$ module since $S = \mathbb{Z}_3 + \sqrt{3}\mathbb{Z}_3$. Furthermore, S is not an integral domain since $\sqrt{3}\sqrt{3} = 3 = 0 \in S$ but $\sqrt{3} \neq 0$. Finally, R is a field and S is not a field since $\sqrt{3}(a+b\sqrt{3}) = a\sqrt{3}+3b = a\sqrt{3} \neq 1$ for $a = 0, 1, 2$.
$\boxed{\Longleftarrow}$ The other direction is true, since if we assume that S is a field, then it must be a commutative integral domain, and so the proof holds.

✌

> **Problem 2.** Suppose R is a commutative unital ring, $\mathfrak{p} \subset R$ is a prime ideal and M is a finitely generated R-module. Recall that the annihilator ideal ${}_R(M)$ consists of elements $r \in R$ such that $rm = 0$ for all $m \in M$. Show the localized module $M_\mathfrak{p}$ is *nonzero* if and only if ${}_R(M) \subset \mathfrak{p}$.

Solution. Since M is finitely generated, there exists $m_1, ..., m_n$ such that

$$M = m_1R + m_2R \cdots + m_nR.$$

$\boxed{\implies}$ Assume M_P is nonzero. Recall that $M_P = S^{-1}M$ where $S = R \backslash P$.

Now, recall that $\frac{m}{s} = 0 \in M_P$ if and only if there exists $t \in S$ so $tm = 0 \in M$.

Assume there exists an $x \in_R (M)$ with $x \notin P$. Then $x \in S$ and since $xm_i = 0 \in M$ for all i, we have that $\frac{m_i}{1} = 0 \in M_P$ for all i and all $s \in S$. Namely, $\frac{m}{s} = 0 \in M_P$ for all $m \in M$ and all $s \in S$ and so $M_P = 0$.

This is a contradiction and so no such x can exist. Namely, ${}_R(M) \subset P$.

$\boxed{\impliedby}$ Assume $\text{Ann}_R(M) \subset P$. Now, assume $M_P = 0$. Then, as stated ealier, for all $m \in M$, there exists $s \in S$ so $sm = 0$.

Namely, for m_i, there exists s_i so $s_im_i = 0$ for all $i = 1, ..., n$.

Let $s = s_1 \cdots s_n$. Then $sm = 0$ for all $m \in M$.

This is clear, since $m \in M$ is of the form $a_1m_1 + \cdots + a_nm_n$ with $a_i \in R$, since M is a finitely generated R-module.

Thus,

$$\begin{aligned} sm &= s\sum_{i=1}^n a_im_i \\ &= \sum_{i=1}^n (s_1 \cdots s_n a_i m_i) \quad = \sum_{i=1}^n (s_1 \cdots s_{i-1}s_{i+1} \cdots s_n a_i s_i m_i) \qquad R \text{ commutative } = \sum_{i=1}^n 0 \\ &= 0 \end{aligned}$$

However, then $s \in \text{Ann}_R(M)$ by definition and since we assumed that $\text{Ann}_R(M) \subset P$, this is a contradiction because $S = R \backslash P$.

Therefore, $M_P \neq 0$.

✌

Problem 3. Let $f(x) = x^5 + 1$. Describe the splitting field K of $f(x)$ over $\mathbb{Q}$ and compute the Galois group $\text{Gal}(K/\mathbb{Q})$.

Solution. The roots z of $f(x)$ all must satisfy that $z^5 = -1$. Thus, if $z = e^{i\theta}$, then $5\theta = \pi, 3\pi, 5\pi, 7\pi, 9\pi$.

Clearly $\xi = e^{i\pi/5}$ is a primitive root, since it generates the others, and so $K = \mathbb{Q}(\xi)$.

Now, we note that -1 is a root of $f(x)$ and dividing out, we see that

$$x^5 + 1x + 1$$

and so

$$x^5 + 1 = (x+1)(x^4 - x^3 + x^2 - x + 1).$$

> **Claim 1.** If A polynomial $f(x)$ is irreducible over $\mathbb{Z}_p$ for any p which does not divide the leading coefficient of f, then $f(x)$ is irreducible over $\mathbb{Q}$.
>
> *Proof.* First, since f is irreducible over $\mathbb{Q}$ if and only if it is irreducible over $\mathbb{Z}$, it suffices to consider $f(x)$ a polynomial over $\mathbb{Z}$.
>
> Now, if f is reducible in $\mathbb{Z}$, then $f(x) = g(x)h(x)$ in $\mathbb{Z}$. However, both g and h have the same degree over $\mathbb{Z}_p$ as they do over $\mathbb{Z}$ since p does not divide the leading coefficient of f, so it cannot divide the leading coefficient of g or h.
>
> Namely, $f(x) = g'(x)h'(x)$ in $\mathbb{Z}_p$ where neither g' nor h' are constant, and so f is reducible over $\mathbb{Z}_p$. ✌

From the claim, over $\mathbb{Z}_2$, $x^4 - x^3 + x^2 - x + 1$ becomes $x^4 + x^3 + x^2 + x + 1$. Now, if this factors into two quadratics, then we would have $(x^2 + ax + b)(x^2 + cx + d)$, with $a, b, c, d = 0, 1$.

Then

$$1 = a + c = b + d + ac = ad + cb = bd.$$

So $b = d = 1$ and either $a = 0$ or $c = 0$. However, then $1 = 1 + 1 + 0 = 0$ which is a contradiction.

Therefore, the polynomial cannot factor into two quadratics, and since all the roots are complex, it cannot factor into linear terms, so the polynomial is irreducible over $\mathbb{Z}_2$ and hence over $\mathbb{Q}$.

Finally, we have that

$$[K : \mathbb{Q}] = 4.$$

Since K is the splitting field of a separable polynomial (all roots are distinct) $K/\mathbb{Q}$ is Galois, and there are only two groups of order 4, so $G = \text{Gal}(K/\mathbb{Q})$ is either $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Now, we note that the roots are exactly, $\xi, \xi^3, \xi^5, \xi^7, \xi^9$. Since $\xi^{10} = 1$, we can rewrite this as $\xi, \xi^3, -1, -\xi^2, -\xi^4$.

Now, $\sigma : K \to K$ defined by $\sigma(\xi) = \xi^3$, defines a map in G.
Furthermore,

$$\sigma^4(\xi) = \sigma^3(\xi^3) = \sigma^2(\xi^9) = \sigma^2(-\xi^4) = \sigma(-\xi^{12}) = \sigma(-\xi^2) = -\xi^6 = \xi$$

and so σ has order 4 and therefore, $G \cong \mathbb{Z}_4$.

✌

Problem 4. Let α be the real positive 16^{th} root of 3 and consider the field $F = \mathbb{Q}(\alpha)$ generated by α over the field of rational numbers. Observe that there is a chain of indeterminate fields

$$\mathbb{Q} \subset \mathbb{Q}(\alpha^8) \subset \mathbb{Q}(\alpha^4) \subset \mathbb{Q}(\alpha^2) \subset \mathbb{Q}(\alpha) = F.$$

Compute the degrees of these intermediate field extensions and conclude they are all distinct. Show that every intermediate field K between $\mathbb{Q}$ and F is one of the above (hint: consider the constant term of the minimal polynomial of α over K).

Solution. The chain is clear. Now,

$$[F : \mathbb{Q}(\alpha^2)] = 2$$

since α clearly satisfies $f(x) = x^2 - \alpha^2 \in \mathbb{Q}(\alpha^2)[x]$. Note that since α is real, it is not possible that $\alpha = a + b\alpha^2$ for any $a, b \in \mathbb{Q}$. Otherwise, α would be a root of $g(x) = bx^2 - x + a$ which is not possible, since α has minimal polynomial $x^{16} - 3$ over $\mathbb{Q}$. Namely, $f(x)$ is the minimal polynomial α satisfies over $\mathbb{Q}(\alpha^2)$.

Similarly,

$$[\mathbb{Q}(\alpha^2) : \mathbb{Q}(\alpha^4)] = [\mathbb{Q}(\alpha^4) : \mathbb{Q}(\alpha^8)] = 2$$

and since $\alpha^{16} = 3$, α^8 satisfies $f(x) = x^2 - 3$ so

$$[\mathbb{Q}(\alpha^8) : \mathbb{Q}] = 2$$

as well.

Therefore, each field in the chain as a proper subfield of the next.

Now, let $\mathbb{Q} \subsetneq K \subsetneq F$. If K contains no powers of α, then $K = \mathbb{Q}$.

Let $\alpha^{2k+1} \in K$ for some $0 < k < 8$. Then

$$(\alpha^{2k+1})^8 = \alpha^{16k+8} = 3^k \alpha^8 \in K$$

so $\alpha^8 \in K$. Therefore,

$$(\alpha^{2k+1})^{2k+1} \alpha^8 = \alpha^{4k^2+4k+8} \alpha = \alpha$$

since $4k^2 + 4k + 8 = 4(k^2 + k + 2) = 16l$ because $k^2 + k + 2$ is an even integer strictly greater than 2 for all non-zero positive integers k.

This is a contradiction, and so K can contain no odd powers of α.

However, now we are basically done. Since $K \neq \mathbb{Q}$, K must contain some even power of α. Let $\alpha^{2k} \in K$ where $0 < k < 8$ is minimal. Then $k = 1, 2, 4$. If $k = 3$, then

$$(\alpha^6)^3 = \alpha^2 = \alpha^{2 \cdot 1}$$

so the minimality of k is contradicted. Similarly, if $k = 5$, then $(\alpha^{10})^2 = \alpha^4 = \alpha^{2\cdot 2}$, and if $k = 6$, then $(\alpha^{12})^2 = \alpha^8 = \alpha^{2\cdot 4}$, and if $k = 7$, then $(\alpha^{14})^2 = \alpha^{12} = \alpha^{2\cdot 6}$ all of which contradict our choice of k.

Therefore, K can only contain powers of α of the form $\alpha^2, \alpha^4, \alpha^8$ and so any intermediate K must be one of the three fields $\mathbb{Q}(\alpha^2), \mathbb{Q}(\alpha^4), \mathbb{Q}(\alpha^8)$.

✌

Problem 5. A finite group is said to be *perfect* if it has nontrivial abelian homomorphic image. Show that a perfect group has no nontrival solvable homomorphac image. Next, suppose that $H \subset G$ is a normal subgroup with G/H perfect. If $\theta : G \to S$ is a homomorphism from G to a solvable group S and if $N = \ker\theta$, show that $G = NH$ and deduce that $\theta(H) = \theta(G)$.

Solution. Assume G is perfect. Let $\varphi : G \to S$ be some group homomorphism such that $\varphi(G) \subset S$ is solvable.

Let K be the kernel of φ. Then $G/K \cong \varphi(G)$ and so G/K is solvable.

Namely, Since $\varphi(G)$ is not abelian, there exists a normal subgroup $N/K \subset G/K$ such that

$$(G/K)/(N/K) \cong G/N \qquad \text{is abelian.}$$

However, then the quotient map $\pi : G \to G/N$ is certainly a surjective homomorphism into an abelian group, which contradicts that G is perfect.

Thus, G can have no solvable homomorphic image.

Now, suppose that G has a normal subgroup H and that G/H is perfect.

Let $\theta : G \to S$ be a homomorphism with S solvable and $N = \ker\theta$. If θ is trivial, then we are done since $N = NH = G$. Assume θ is non-trivial.

Then $G/N \cong \theta(G)$ which is solvable since subgroups of solvable groups are also solvable.

Now, let $f : G/H \to \theta(G)$ defined by $f(gH) = \theta(g)$. Then f is well defined since if $gH = g'H$, then $g = g'h$ for some $h \in H$ so $f(gH) = f(g'hH) = f(g'H)$.

Now, since G/H is perfect, f must be the zero map. Namely, $\theta(g) = 0$ for all $gH \in G/H$.

Thus, $\theta(g) = 0$ for all $g \notin H$. Therefore, if $g \notin H$, then $g \in N$.

Since N is normal, NH is a subgroup of G and since any $g \notin H$ implies $g \in N$, and G is finite, $G = NH$. ✌

Problem 6. Let A be a finite dimensional $\mathbb{C}$-algebra. Given $a \in A$, write L_a for the left multiplication operatire, i.e., $L_a(b) = ab$. Define a map $(-,-) : A \times A \to \mathbb{C}$ by means of the formula $(a,b) := \operatorname{tr}(L_a L_b)$.

(a) Show that $(-,-)$ is a symmetric bilinear form on A.

(b) If one defines the radical $\operatorname{Rad}(-,-)$ as $\{a \in A \,|\, (a,b) = 0 \forall b \in A\}$, then show that $\operatorname{Rad}(-,-)$ is a two-sided ideal in A.

(c) Show that $\operatorname{Rad}(-,-)$ coincides with the Jacobson radical of A.

Solution.

(a) First, we note that

$$L_{ab}(x) = abx = aL_b(x)$$

for all $a, b, x \in A$ and

$$L_{a+b}(x) = (a+b)x = ax + bx = L_a(x) + L_b(x)$$

Therefore, since the trace is a linear operation, for $a \in \mathbb{C}$ and $x, y, z \in A$, we have that

$$\begin{aligned}
(ax + ay, z) &= \operatorname{tr}(L_{ax+ay} L_z) \\
&= \operatorname{tr}((L_{ax} + L_{ay}) L_z) \\
&= \operatorname{tr}((aL_x + aL_y) L_z) \\
&= a\operatorname{tr}(L_x L_z) + a\operatorname{tr}(L_y L_z) \\
&= a(x,z) + a(y,z)
\end{aligned}$$

and similarly

$$(z, ax + ay) = a(z,x) + a(z,y).$$

Therefore, $(-,-)$ is bilinear. It is symmetric, since $\operatorname{tr}(AB) = \operatorname{tr}(BA)$ so

$$(x,y) = \operatorname{tr}(L_x L_y) = \operatorname{tr}(L_y L_x) = (y,x).$$

(b) Let $x, y \in \operatorname{Rad}(-,-)$. Then

$$(x - y, b) = (x,b) - (y,b) = 0 - 0 = 0$$

for all $b \in A$ so $x - y \in \operatorname{Rad}(-,-)$.

Similarly, if $r \in A$ then $(rx, b) = (x, rb) = 0$ for all $b \in A$ so $rx \in \operatorname{Rad}(-,-)$ and $(xr, b) = (x, rb) = 0$ for all $r \in A$.

Therefore, $\operatorname{Rad}(-,-)$ defines an ideal in A.

(c) Since A is finite dimensional, it is Artinian, so $J(A)$ is nilpotent.

let $x \in J(A)$. Then for all $b \in A$, $xb \in J(A)$ since $J(A)$ is a 2-sided ideal. Now, there exists an n so $(xb)^n = 0$ since $J(A)$ is nilpotent so

$$L_{(xb)^n} = (L_{xb})^n = 0.$$

So L_{xb} is nilpotent. Since nilpotent matrices always have zero-trace,

$$(x, b) = (xb, 1) = \mathrm{tr}(L_{xb}) = 0.$$

And since $b \in A$ was arbitrary, then $x \in \mathrm{Rad}(-, -)$.

> Recall: If a matrix M is nilpotent, then $M^n = 0$ for some n. Let λ be an eigenvalue of M and v a non-zero eigenvector. Then $M^n v = \lambda^n v = 0$ so $\lambda = 0$. Thus, M has only zero eigenvalues, and since $\mathrm{tr}(M)$ is the sum of the eigenvalues, $\mathrm{tr}(M) = 0$.

Let $a \in \mathrm{Rad}(-, -)$. Then, we note that $(a^n, 1) = \mathrm{tr}(L_{a^n}) = \mathrm{tr}(L_a^n) = 0$ for all n, so $\sum_{i=1}^n \lambda_i^n = 0$ for all n, where λ_i are the (not necessarily distinct) eigenvalues of L_a.

Now, we note that if characteristic polynomial of L_a is $p(x)$, then $p(x) = \prod_{i=1}^n (x - \lambda_i)$ and by Cayley Hamilton, L_a satisfies $p(x)$.

Since $p(x)$ is a polynomial with coefficeints that are symmetric in λ_i and since $\sum_{i=1}^n \lambda_i^n = 0$ for all n implies that all the symmetric polynomials in the λ_i are 0, we have that $p(x) = x^n$.

Namely, L_a has only 0 as an eigenvalue and so it is nilpotent.

Thus, there exists an n such that $L_{a^n} = L_a^n = 0$. Therefore, $a^n 1 = a^n = 0$ so a is nilpotent.

Since all nilpotent elements are quasi-regular and since $J(R)$ is the largest quasi-regular 2-sided ideal, it must be that $\mathrm{Rad}(-, -) \subset J(R)$.

✌

Problem 7. Suppose F is an algebraically closed field, V is a finite-dimensional F-vector space, and $A \in \text{End}_F(V)$. Show that there exists polynomial $f, g \in F[x]$ such that

(i) $A = f(A) + g(A)$

(ii) $f(A)$ is diagonalizable and $g(A)$ is nilpotent

(iii) f and g both vanish at 0.

Solution. Let
$$p_A(x) = \prod_{i=1}^{m}(x-\lambda_i)^{k_i}$$
be the minimal polynomial of A. If x divides $p(x)$, then let $p(x) = p_A(x)$ else we let $p(x) = xp_A(x)$ and WLOG, let $\lambda_0 = 0$.

Let
$$q_i(x) = \frac{p(x)}{(x-\lambda_i)^{k_i}} \qquad i = 0, ..., m$$
Note that $q_i(A) \neq 0$ since q_i has degree strictly smaller than p. Then for all $i \neq j$, q_i and $(x-\lambda_i)^{k_i}$ are coprime, and so there exists polynomials $a_i(x)$ so
$$1 = \sum_{i=0}^{m} f_i(x) \qquad f_i(x) = a_i(x)q_i(x).$$

Now, let
$$f(x) = \sum_{i=0}^{m} \lambda_i f_i(x).$$

Then,
$$\lambda_j I - f(A) = \lambda_j \sum_{i=0}^{m} f_i(A) - \sum_{i=0}^{m} \lambda_i f_i(A) = \sum_{i=0}^{m}(\lambda_j - \lambda_i) f_i(A).$$

Next, since $p_A(x)$ divides $q_i(x)q_j(x)$ for all $i \neq j$, we have that $f_i(A)f_j(A) = 0$ for all $i \neq j$. Namely,
$$f_j(A) = f_j(A)\sum_{i=0}^{m} f_i(x) = f_j(A)^2$$
for all j.

Therefore,
$$f^2(A) = \left(\sum_{i=0}^{m} \lambda_i f_i(A)\right)^2 = \sum_{i=0}^{m} \lambda_i^2 f_i^2(A)$$

Thus,

$$\begin{aligned}(\lambda_j I - f(A))(\lambda_k I - f(A)) &= \lambda_j\lambda_k I - (\lambda_j + \lambda_j)f(A) + f^2(A)\\ &= \lambda_j\lambda_k \sum_{i=0}^m f_i(A) - (\lambda_j + \lambda_k)\sum_{i=0}^m \lambda_i f_i(A) + \sum_{i=0}^m \lambda_i^2 f_i^2(A)\\ &= \sum_{i=0}^m (\lambda_j\lambda_k - (\lambda_j+\lambda_k)\lambda_i + \lambda_i^2) f_i(A)\\ &= \sum_{i=0}^m (\lambda_j - \lambda_i)(\lambda_k - \lambda_i) f_i(A)\end{aligned}$$

Finally,

$$\prod_{i=0}^m (f(A) - \lambda_j I) = \sum_{i=1}^m \prod_{i=0}^m (\lambda_j - \lambda_i) f_i(A) = 0$$

since there is a $\lambda_j - \lambda_j = 0$ term in every product.

Thus, $f(A)$ has minimal polynomial dividing $\prod_{i=0}^m (x - \lambda_j)$, and since if v is an eigenvector of A associated to eigenvalue λ_i, then $f(A)v = \lambda_i v$ by construction. Therefore, $f(A)$ has the same eigenvalues as A and is diagonalizable.

Finally, let $g(x) = x - f(x)$. Then

$$g(A) = A - f(A) = \sum_{i=1}^m (A - \lambda_i I) f_i(A).$$

Then, let

$$k = \max_{i=0,\dots,m} k_i.$$

Then

$$g^k(A) = (A - f(A))^k = \sum_{i=1}^m (A - \lambda_i I)^k f_i(A) = 0$$

since $p_A(x)$ divides $(A - \lambda_i I)^k f_i(A)$.

At last, we have that

$$A = f(A) + g(A)$$

where $f(A)$ is diagonalizable and $g(A)$ is nilpotent, and by construction, f and g both vanish at 0. ✌