MATH 101: ALGEBRA I
FINAL EXAM SOLUTIONS

Problem 1. Let F be a field. For a group G written multiplicatively, recall that the group algebra $F[G]$ is the F-vector space with basis G and multiplication induced by the group law in G, extended F-linearly.

Let $G = S_3$, let $\tau = (1\ 2)$, and let $\alpha = 1 + \tau \in F[G]$.

(a) The element α acts F-linearly by left multiplication on $F[G]$:

$$\begin{aligned} T : F[G] &\to F[G] \\ \beta &\mapsto \alpha\beta \end{aligned}$$

Compute the matrix of T with respect to a basis of elements of G.

(b) Compute the minimal polynomial and characteristic polynomial of T.

(c) Let $B = F[G]$, let $I = \{\alpha\beta : \beta \in B\}$ be the right ideal of B generated by α. Observe that I and B/I are F-vector spaces, and compute $\dim_F I$ and $\dim_F(B/I)$.

Solution. For (a), let $\sigma = (1\ 2\ 3)$. Then $\tau\sigma = (1\ 2)(1\ 2\ 3) = (2\ 3)$ and $\tau\sigma^2 = (1\ 2)(1\ 3\ 2) = (1\ 3)$. Therefore in the basis

$$1, \tau, \sigma, \tau\sigma, \sigma^2, \tau\sigma^2 = (), (1\ 2), (1\ 2\ 3), (2\ 3), (1\ 3\ 2), (1\ 3)$$

we compute

$$\begin{aligned} \alpha 1 &= \alpha = 1 + \tau \\ \alpha\tau &= (1+\tau)\tau = \tau + \tau^2 = 1 + \tau \\ \alpha\sigma &= (1+\tau)\sigma = \sigma + \tau\sigma \\ &\dots \end{aligned}$$

which gives the matrix

$$[T] = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

For (b), because $[T]$ is a block matrix, the minimal polynomial of T is the same as the minimal polynomial of a block $B = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$; this matrix satisfies $f(x) = x^2 - 2x = x(x-2)$ and is not a scalar matrix, so $f(x)$ is the minimal polynomial. The characteristic polynomial is $f(x)^3 = x^3(x-2)^3$.

For (c), it is clear that I is a right ideal; and from above, we see that the image of multiplication by α has dimension 3, so $\dim_F I = 3$, and by rank-nullity $\dim_F F[G]/I = \dim_F F[G] - \dim_F I = 6 - 3 = 3$ as well.

Problem 2. Let $n \in \mathbb{Z}_{\geq 1}$. Let $A \in \mathrm{GL}_n(\mathbb{C})$ have n distinct eigenvalues $\lambda_1, \dots, \lambda_n$. Let $V = \mathrm{M}_n(\mathbb{C})$. Find the eigenvalues of the $\mathbb{C}$-linear map

$$\begin{aligned} T : V &\to V \\ M &\mapsto AMA^{-1}. \end{aligned}$$

Date: Tuesday, 22 November 2016.

Solution. Note $A \in \mathrm{GL}_n(\mathbb{C})$ implies $\lambda_i \in \mathbb{C}^\times$. Since A has n distinct eigenvalues, it is diagonalizable, and there is a matrix $P \in \mathrm{GL}_n(\mathbb{C})$ such that $PAP^{-1} = \mathrm{diag}(\lambda_1, \dots, \lambda_n) = D$. Let E_{ij} be the matrix unit with 1 in the ith row and jth column; then E_{ij} is a basis for V, with $1 \le i, j \le n$. We compute

$$DE_{ij}D^{-1} = \lambda_i \lambda_j^{-1} E_{ij}$$

so for $A = D$ we have n^2 eigenvalues $\lambda_i\lambda_j^{-1}$ with $1 \le i, j \le n$. But these are also the n^2 eigenvalues for T by taking the basis $P^{-1}E_{ij}P$ instead (check directly still a basis): since

$$AMA^{-1} = P^{-1}D(PMP^{-1})D^{-1}P$$

we have

$$AP^{-1}E_{ij}PA^{-1} = P^{-1}DE_{ij}D^{-1}P = \lambda_i\lambda_j^{-1}P^{-1}E_{ij}P.$$

Problem 3. Let p be an odd prime, and let $G = \mathrm{GL}_2(\mathbb{F}_p)$.

(a) Prove that a p-Sylow subgroup of G is cyclic, and exhibit a p-Sylow subgroup of G.
(b) Give two different reasons why every p-Sylow subgroup of G is conjugate to the one given in (a), at least one of which implies that any two *generators* of two p-Sylow subgroups are conjugate.
(c) Show that there are exactly $p + 1$ distinct p-Sylow subgroups in G.

Solution. For (a), we have $\#\,\mathrm{GL}_2(\mathbb{F}_p) = (p^2 - 1)(p^2 - p) = p(p-1)^2(p+1)$, so $p \parallel \#G$, and a group of prime order is cyclic. To exhibit a p-Sylow subgroup, we need only find an element of order p: the matrix $J = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ will do.

For (b): the first reason is Sylow's theorem, which says that all Sylow p-subgroups are conjugate; the second reason is because any generator of a p-Sylow subgroup is not scalar and satisfies $x^p = 1$ so $x^p - 1 = (x-1)^p = 0$, so its minimal polynomial is $(x-1)^2$ (it cannot a scalar matrix, since such a matrix has order dividing $p - 1$) and therefore is conjugate to the matrix J.

Now (c). First proof. The p-Sylow subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$ are the same as the p-Sylow subgroups of $\mathrm{SL}_2(\mathbb{F}_p)$: an element of order p necessarily has determinant 1. By Sylow's theorem we know that the number n_p of p-Sylow subgroups has $n_p \equiv 1 \pmod p$ and $n_p \mid \#\,\mathrm{SL}_2(\mathbb{F}_p)/p = (p-1)(p+1)$. We can see that $n_p > 1$, since we could also take the lower triangular subgroup in place of J, so $n_p \ge p + 1$. Now Write $n_p = 1 + kp \ge 1 + p$ so that $(1 + kp)d = p^2 - 1$ for some $d \in \mathbb{Z}_{>0}$; then $d \equiv -1 \pmod p$, so $d \ge p - 1$. But that already maxes us out: we must have $d = p - 1$ and $n_p = p + 1$.

Second proof: by (b), the group $\mathrm{GL}_2(\mathbb{F}_p)$ acts transitively by conjugation on the set X of elements of order p. By the orbit-stabilizer formula, we have $\#X = \#G/\#\,\mathrm{Stab}_G(J)$. The linear algebra calculation $AJ = JA$ shows that

$$A \in \mathrm{Stab}_G(J) = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a \in \mathbb{F}_p^\times, b \in \mathbb{F}_p \right\}$$

with $\#\,\mathrm{Stab}_G(J) = p(p-1)$, so $\#X = (p-1)(p+1)$. There are $p - 1$ generators of each p-Sylow subgroup, so the total number is $p + 1$.

Third proof (really the same as second proof): by the first part of (b), as for any group, G acts transitively by conjugation on $\mathrm{Syl}_p(G)$; the stabilizer of a subgroup $H \in \mathrm{Syl}_p(G)$ is the normalizer $\mathrm{N}_G(H)$, so $n_p(G) = \#G/\#N_G(H)$. Now compute $AJ = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} A$ to see that

$$\mathrm{N}_G(H) = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, c \in \mathbb{F}_p^\times, b \in \mathbb{F}_p \right\}$$

of order $p(p-1)^2$, and conclude again that $n_p(G) = p + 1$.

Problem 4. Let k be a field and let $R = k[x, y]$ be the polynomial ring over k in the variables x, y.

(a) Show that the ideal $(x) \subseteq R$ generated by x is a projective R-module.
(b) Show that the ideal (x, y) generated by both x, y is *not* a projective R-module. *[Hint: Show that the surjective R-module homomorphism $\phi : R^2 \to (x, y)$ defined by $\phi(e_1) = x$ and $\phi(e_2) = y$ does not split, where e_1, e_2 is the standard basis for R^2.]*

Solution. For (a), $(x) = xR$ is free, so projective.

For (b), we take the hint and the map ϕ. Let $I = (x, y)$. Suppose that $\mu : I \to R^2$ is a splitting, so μ is an R-module homomorphism with $\phi\mu = \mathrm{id}_I$. Let $\mu(x) = ae_1 + be_2 \in R^2$ and $\mu(y) = ce_1 + de_2 \in R^2$. Then

$$x = (\phi\mu)(x) = \phi(ae_1 + be_2) = ax + by$$

(and similarly $y = cx + dy$). But also

$$\mu(xy) = x\mu(y) = y\mu(x) = aye_1 + bye_2 = cxe_1 + dxe_2.$$

Thus $by = dx$ and $ay = cx$. Since R is a UFD and x, y are nonassociate irreducibles (by degree), we have $x \mid a$ and $x \mid b$; therefore $x = (a/x)x^2 + (b/x)xy$, and since R is a domain, we conclude $1 = (a/x)x + (b/x)y$. Therefore $1 \in (x, y)$, a contradiction. Since there is no splitting, (x, y) cannot be a projective R-module.

Problem 5. Let $R = \mathbb{Z}[i]$ where $i^2 = -1$.

(a) Compute a generator of the ideal $(3 + 11i, 1 + 3i)$.

(b) Let M be the R-module generated by x_1, x_2, x_3 subject to the relations

$$(i + 1)x_2 + (i - 1)x_3 = 0$$
$$6x_1 + (3i - 1)x_2 - (i + 9)x_3 = 0$$

Compute the rank of M and the invariant factors of the torsion submodule $\mathrm{Tor}(M)$.

Proof. For (a), we use the Euclidean algorithm for $\mathbb{Z}[i]$: we have $(3+11i)/(1+3i) = (18+i)/5$ which rounds to 4, and $3 + 11i - 4(1 + 3i) = -i - 1$, and $(1 + 3i)/(1 + i) = i + 2$ so $1 + i$ is a generator.

We compute the Smith normal form using row and column operations over $\mathbb{Z}[i]$ to get

$$\begin{pmatrix} 1+i & 0 & 0 \\ 0 & 6 & 0 \end{pmatrix}$$

which implies that $M \simeq R/(1 + i) \oplus R/(6) \oplus R$ (adding a superfluous zero relation); the rank is 1 and the invariant factors are $(1 + i) \mid (6)$. $\square$

Problem 6. Let R be a commutative ring and let M, N be R-modules.

(a) State the universal property of $M \otimes_R N$.

(b) Suppose that R is a domain with field of fractions F, and that $N \subseteq M$ is an R-submodule such that M/N is a torsion R-module. Show that the inclusion $N \hookrightarrow M$ induces an F-vector space isomorphism

$$N \otimes_R F \xrightarrow{\sim} M \otimes_R F.$$

Solution. Part (a) is standard. For (b), we define a map $N \times F \to M \otimes_R F$ by $(y, a) \mapsto y \otimes a$; this map is R-bilinear, so by the universal property we have an R-module homomorphism $N \otimes_R F \to M \otimes_R F$. This map is further an F-vector space map: it is still linear, and we can just as easily scale in the F-component. We can then argue with linear algebra over F to show it is an isomorphism; we find it easier to define an inverse map as follows. We define a map $\psi : M \times F \to N \otimes_R F$ in the following way: let $(x, a) \in M \times F$. Then M/N is torsion, so there exists nonzero $r \in R$ such that $rx \in N$; we define $\psi(x, a) = (rx) \otimes (ar^{-1}) \in N \otimes_R F$. This map is well-defined: if $sx \in N$, then

$$rs(sx \otimes as^{-1}) = sx \otimes ar = rsx \otimes a = rx \otimes as = rs(rx \otimes ar^{-1})$$

so since $N \otimes_R F$ is a vector space and $rs \neq 0$, we have $sx \otimes as^{-1} = rx \otimes ar^{-1}$. By the universal property, we get an R-module homomorphism ψ and then an F-vector space map. It is routine then to check that the composition of these two maps in either direction is the identity.

If you're willing to take for granted things some things we proved in class, this can be made a bit faster, at least when M, N are finitely generated: when M/N is torsion, we showed that M and N have the same rank (maximal cardinality of a linearly independent set), and that $\mathrm{rk}_R M = \dim_F(M \otimes_R F)$, indeed, the linearly independent over R (and spanning) implies linearly independent over F (and spanning). See the next paragraph for the fast proof that the map is surjective; it is then an isomorphism by dimensions.

(Final, more 'advanced' proof: F is flat over R, so the inclusion ϕ gives an injection $\phi \otimes 1 : N \otimes_R F \hookrightarrow M \otimes_R F$. The map is surjective: it is enough to show this on simple tensors, and just as above, given $x \otimes a$ and $rx \in N$, we have $r(x \otimes a) = rx \otimes a \in \operatorname{img} \phi$, so since $\operatorname{img} \phi$ is an F-vector space, we have $x \otimes a \in \operatorname{img} \phi$.)