# Math 30820 Honors Algebra 4
# Homework 2

Andrei Jorza

Due Wednesday, 2/1/2017

**Do 6 of the following questions. Some questions may be obligatory. Artin a.b.c means chapter a, section b, exercise c. You may use any problem to solve any other problem.**

1. (You have to do this problem) Suppose $R$ is a commutative ring with unit and $M$ is an $R$-module. Define the annihilator of $M$ in $R$ as $\mathrm{Ann}_R(M) = \{r \in R \mid rm = 0, \forall m \in M\}$.

   (a) Show that $\mathrm{Ann}_R(M)$ is an ideal of $R$.

   (b) Show that if $I \subset \mathrm{Ann}_R(M)$ is an ideal of $R$ then $M$ is naturally an $R/I$-module.

   (c) What is $\mathrm{Ann}_R(R/I)$?

   *Proof.* (a): If $x, y \in \mathrm{Ann}_R(M)$ and $r \in R$ then $xm = ym = 0$ for all $m \in M$ so $(x+ry)m = xm+rym = 0$ and so $x + ry \in \mathrm{Ann}_R(M)$. We deduce that $\mathrm{Ann}_R(M)$ is an ideal.

   (b): If $I \subset \mathrm{Ann}_R(M)$ and $r + I \in R/I$ and $m \in M$ define $(r + I)m = rm \in M$. If $r' + I = r + I$ then $r' - r \in I \subset \mathrm{Ann}_R(M)$ and so $r'm - rm = (r' - r)m = 0$ which means that this scalar operation is well-defined. It's easy to check that it is an actual scalar multiplication on $M$ and so $M$ is an $R/I$-module.

   (c): We're asking for what $x \in R$ is it the case that $xy = 0$ for all $y \in R/I$. In particular we'd need $x = 0$ and so $x \in I$. If $x \in I$ then $xy \in I$ and so $xy = 0$ in $R/I$. Thus $\mathrm{Ann}_R(R/I) = I$. □

2. Show that the integral domain $R = \mathbb{C}[X^2, X^3]$ is not *integrally closed*, i.e., that there exists an element $\alpha \in \mathrm{Frac}\, R$ such that $\alpha \notin R$ and $\alpha$ is integral over $R$.

   *Proof.* Note that $X = X^3/X^2 \in \mathrm{Frac}\, R$ and is a root of the polynomial $P(Y) = Y^2 - X^2 \in R[Y]$ so $X$ is integral. To show that $X \notin R$ suppose that $X = P(X^2, X^3)$ for some polynomial in two variables with complex coefficients. Taking derivatives we get $1 = 2XP(X^2, X^3) + 3X^2P(X^2, X^3)$ and the RHS vanishes at 0. □

3. Let $F$ be a field and $A \in M_{n\times n}(F)$ be a matrix. Recall that in class we defined the following $F[X]$-module $M_A$: as an abelian group $M_A = F^n$ and scalar multiplication is given by $P(X) \cdot v := P(A)v$ where $P(A) \in M_{n\times n}(F)$ and $F^n$ is interpreted as $M_{n\times 1}(F)$. Suppose $S \in \mathrm{GL}(n, F)$. Show that $M_A \cong M_{SAS^{-1}}$ as $F[X]$-modules.

   *Proof.* Consider the map $\phi : M_A \to M_{SAS^{-1}}$ given by $\phi(v) = Sv$. We need to check that it is an isomorphism of $F[X]$-modules. First, since $S$ is invertible it is an isomorphism of $F$-vector spaces so $\phi$ is bijective and is additive. We only need to check that $\phi$ is a homomorphism of $F[X]$-vector spaces and since we already know additivity we only need that $P(X) \cdot_{M_{SAS^{-1}}} \phi(v) = \phi(P(X) \cdot_{M_A} v)$ for all $P \in F[X]$ and $v \in M_A$.

   $$P(X) \cdot_{M_{SAS^{-1}}} \phi(v) = P(SAS^{-1})Sv = SP(A)S^{-1}Sv = SP(A)v = \phi(P(A)v) = \phi(P(X) \cdot_{M_A} v)$$

   where I used the fact that $P(SAS^{-1}) = SP(A)S^{-1}$ from last semester. □

4. Artin 14.1.4 on page 437.

   *Proof.* (a): Pick $m \in M$ nonzero. Then $Rm \subset M$ is a nonzero submodule on $M$ and by simplicity $M = Rm$. Therefore $R \to M$ given by $f(x) = xm$ is surjective and so $M \cong R/\ker f$ by the first isomorphism theorem. Since $I = \ker f \subset R$ is a submodule it is an ideal and it remains to show that $I$ is a maximal ideal. If it is not maximal it follows that $R/I$ is not a field so there exists $0 \neq r \in R/I$ which is not invertible. But then the principal ideal $(r)$ of $R/I$ is a submodule of $R/I$ and simplicity of $R/I$ implies that either $(r) = 0$ (assumed to not be true) or $(r) = R/I$ which would imply $r$ is invertible in $R/I$.

   (b): From class $\ker \phi$ is a submodule of $S$, which is simple. Either $\ker \phi = 0$ in which case $\phi$ is injective or $\ker \phi = 0$ in which case $\varphi = 0$. Now $\operatorname{Im} \phi$ is a submodule of the simple module $S'$. Either $\operatorname{Im} phi = 0$ in which case $\phi = 0$ or $\operatorname{Im} \phi = S'$ in which case $\phi$ is surjective. Therefore either $\phi = 0$ or $\phi$ is an isomorphism. □

5. Artin 14.2.3 (a) and from (b) the "only if" part on page 437.

   *Proof.* (a): If $\phi : \mathbb{Z}^n \to \mathbb{Z}^m$ is given by the matrix $A$ then the matrix $A \in M_{m,n}(\mathbb{Z}) \subset M_{m,n}(\mathbb{R})$ also yields a linear map $\phi_{\mathbb{R}} : \mathbb{Q}^n \to \mathbb{Q}^m$. If $\phi$ is not injective neither is $\phi_{\mathbb{Q}}$ because if $\phi_{\mathbb{Q}}(v) = 0$ for a nonzero $v \in \mathbb{Q}^n$ then we can clear denominators in $v$ to get a nonzero integral $Nv$ with $\phi(Nv) = 0$. If $\det A \neq 0$ then $\phi_{\mathbb{R}}$ is injective and therefore so is $\phi$.

   (b): If $\phi$ has matrix $A$ and $p$ is any prime let $\phi_p : \mathbb{F}_p^n \to \mathbb{F}_p^m$ be the linear map obtained from the matrix $\overline{A} = A \mod p \in M_{m,n}(\mathbb{F}_p)$. If $\phi$ is surjective then so is $\phi_p$ because if $\overline{v} \in \mathbb{F}_p^m$ and $v \in \mathbb{Z}^m$ is any vector with $v \mod p = \overline{v}$ then $\phi(u) = v$ for some $u \in \mathbb{Z}^n$ and immediately $\phi_p(u \mod p) = \overline{v}$. Now if the $m \times m$ minors of $A$ were not coprime we could choose a prime divisor $p$ of all these determinants. But then the matrix $\overline{A}$ would have rank $< m$ which would contradict the fact that $\phi_p$ is surjective as $\dim_{\mathbb{F}_p} \operatorname{Im} \phi_p = \operatorname{rank} \overline{A}$ from linear algebra over fields.

   □

6. Artin 14.2.4 on page 437.

   *Proof.* (a): If $I = (a)$ is principal then $I$ has a basis and so $I$ is free. If $I$ is not principal but free it has a basis with at least two vectors and let $a, b \in I$ be two such basis vectors of $I$. But then $ab + b(-a) = 0$ so $a$ and $b$ are dependent over $R$ contradicting the fact they form a basis.

   (b): $R/0 = R$ is free and $R/R = 0$ is free. Suppose $R/I$ is free for $I \neq 0, R$. Pick $u \in R/I$ any basis vector. But then $xu = 0$ whenever $x \in I$ so $u$ has a linear dependence. □

7. Artin 14.7.9 on page 439.

   *Proof.* If $M$ is a $\mathbb{Z}[i]$-module define the abelian group $V = M$ and $\phi : V \to V$ as $\phi(v) = iv \in V$. Then $\phi$ is an $R$-module homomorphism and so it is a homomorphism of abelian groups. Moreover, $\phi \circ \phi(v) = i^2 v = -v$ and so $\phi \circ \phi = -\operatorname{id}_V$.

   Reciprocally, suppose $V$ and $\phi$ are given as in the problem. Define $M = V$ as an abelian group and define scalar multiplication by $R$ as

   $$(a + bi)v = av + b\phi(v)$$

   This is well-defined and visibly satisfies $r(v + w) = rv + rw$ as $\phi$ is a linear map. Moreover, $(rs)v = r(s(v))$ by computations as

   $$(a+bi)((c+di)v) = (a+bi)(cv+d\phi(v)) = a(cv+d\phi(v))+b\phi(cv+d\phi(v)) = (ac-bd)v+(ad+bc)\phi(v) = ((a+bi)(c+di))v$$

   as $\phi \circ \phi = -\operatorname{id}_V$. □

8. Artin 14.8.2 on page 440. (Here the "corresponding linear operator" refers to multiplication by $t$.)

*Proof.* Let $1, t-\alpha, (t-\alpha)^2, \ldots, (t-\alpha)^{n-1}$ be a basis of $\mathbb{C}[t]/(t-\alpha)^n$ over $\mathbb{C}$. Multiplication by $t$ in this basis satisfies

$$t(t-\alpha)^i = (t-\alpha)^{i+1} + \alpha(t-\alpha)^i$$

and so the matrix of multiplication by $t$ is a full Jordan block with $\alpha$ on the diagonal. □