Math 122 Fall 2014 Solutions to Practice Problems for Final

Practice Problems for matrices and Cayley-Hamilton

1. Basics in characteristic polynomials

(a) Let F be a field, and A a $k \times k$ matrix with entries in F. Show that A is not conjugate to an upper-triangular matrix unless its characteristic polynomial can be factored into (possibly non-distinct) linear polynomials in $F[t]$.
(b) Given an example of a matrix in a field F whose characteristic polynomial cannot be factored into linear polynomials.
(c) Prove that if A is a $k \times k$ matrix with entries in a field F, its characteristic polynomial $\Delta(t)$ is a degree k polynomial in $F[t]$, and that the degree $k-1$ coefficient of $\Delta(t)$ is $-\text{tr}(A)$. (Here, $\text{tr}(A)$ is the trace of A—the sum of its diagonal entries.)
(d) Prove that the constant term of $\Delta(t)$ is $(-1)^k \det A$.

(a) Suppose that A is conjugate to an upper-triangular matrix, so $T = BAB^{-1}$ where T is upper-triangular and B is invertible. Recall the characteristic polynomial of T and A are the same, because

$$\det(tI-T) = \det(tI-BAB^{-1}) = \det(B(tI-A)B^{-1}) = \det B \det B^{-1}(tI-A) = \det(tI-A).$$

On the other hand,

$$tI - T = \begin{bmatrix} t-T_{11} & -T_{12} & \dots & -T_{1k} \\ 0 & t-T_{22} & \dots & -T_{2k} \\ 0 & 0 & \dots & \vdots \\ 0 & 0 & \dots & t-T_{kk} \end{bmatrix}$$

is an upper-triangular matrix, so its determinant is given by multiplying its diagonal entries:

$$\det(tI-T) = (t-T_{11})\dots(t-T_{kk})$$

so the characteristic polynomial of A factors into linear polynomials.

(b) Let us choose $\mathbb{R} = F$ to be our field. We know $\mathbb{R}$ has no square root of -1, so we reverse-engineer a matrix whose characteristic polynomial is $t^2+1=0$. For instance,

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

(c) For a field F, consider an injective ring homomorphism $F \hookrightarrow \overline{F}$ into an algebraically closed field $\overline{F}$. Any matrix $A \in M_{k\times k}(F)$ is conjugate to an upper-triangular matrix with entries in $\overline{F}$ (by the classification of finitely generated modules over PIDs). And the characteristic polynomial of an upper-triangular matrix is

$$\det(tI - T) = (t - T_{11})\dots(t - T_{kk})$$

which is clearly a degree k polynomial. Moreover, the characteristic polynomial of A is unchanged by conjugation, so we conclude that the characteristic polynomial of A is also degree k. (Note that each linear factor, $t - T_{ii}$, is a polynomial in $\overline{F}[t]$, but may not be a polynomial in $F[t]$.) To prove the statement about trace: Note that the degree $k-1$ portion of the above polynomial is given by

$$-T_{11} - \dots - T_{kk} = -tr(T).$$

But trace is also left unchanged by conjugation. Here is a two-step proof: First,

$$\mathrm{tr}(AB) = \sum_{i=1}^{k}(AB)_i i = \sum_{i=1}^{k}\sum_{j=1}^{k} A_{ij}B_{ji} = \sum_{i=1}^{k}\sum_{j=1}^{k} B_{ji}A_{ij} = \sum_{j=1}^{k}\sum_{i=1}^{k} B_{ji}A_{ij} = \sum_{j=1}^{k}(BA)_{jj} = \mathrm{tr}(BA).$$

Plugging in $B = D^{-1}C$ and $A = D$, we see that

$$\mathrm{tr} D^{-1}CD = \mathrm{tr} C$$

Since the trace of T is given by $-\mathrm{tr}(T)$, the trace of the original matrix is also given by negative its trace.

(d) Here are two proofs: Again, use that determinants are also unchanged by conjugation. So $\det(A) = \det(T)$ if T is an upper-triangular matrix conjugate to A. The constant term of $(t - T_{11})\dots(t - T_{kk})$ is obviously $(-1)^k \det T$ (since it is the product of the diagonal entries of T) so the constant term of $\det(tI - A)$ is also $(-1)^k \det T = (-1)^k \det A$. For a second proof, recall that if $f : R \to S$ is a ring homomorphism, and if $F : M_{k\times k}(R) \to M_{k\times k}(S)$ is the induced map on matrices, then $f(\det A) = \det F(A)$ for every matrix A. Evaluating a polynomial at $t = 0$ is a ring homomorphism from $F[t] \to F$, so given the characteristic polynomial of $tI - A$, we have that

$$\det(0I - A) = \det(-A) = (-1)^k A.$$

On the other hand, evaluating any polynomial at $t = 0$ simply recovers the constant term of the polynomial.

2. Matrices are linear transformations

Let R be a commutative ring and $R^{\oplus k}$ the free module on k generators. Show there is a ring isomorphism

$$T : M_{k\times k}(R) \to \hom_R(R^{\oplus k}, R^{\oplus k})$$

given by sending a matrix A to the homomorphism T_A sending the ith standard basis element of $R^{\oplus k}$ to the element

$$\sum_{j=1}^{k} A_{ji} e_j.$$

If you are lazy and don't want to do every part of the proof, here is the most important part: prove that $T_{AB} = T_A \circ T_B$, so that matrix multiplication is sent to composition of functions.

Remark 2.1. (Recall that a homomorphism from $R^{\oplus k}$ to any module M is determined by the choice of k elements $x_1, \ldots, x_k$ in M, simply be declaring that $e_i \in R^{\oplus k}$ get sent to x_i.)

Remark 2.2. To be clear, the target of T is the set of all left R-module homomorphisms from $R^{\oplus k}$ to itself.

Remark 2.3. By the way, this ring isomorphism is the justification for saying that a linear map from a finite-dimensional vector space over F to itself is the same thing as a matrix—in this case, $R = F$, and every finite-dimensional vector space over F is isomorphic to $F^{\oplus k}$ for some k.

Let e_i denote the ith standard basis element of $R^{\oplus k}$—it is the element which has the multiplicative unit 1 in the ith coordinate, and 0 elsewhere. Let A be a matrix. By definition, T assigns to A the linear transformation taking e_i to the element

$$\sum_{j=1}^{k} A_{ji} e_j \in R^{\oplus k}.$$

This defines the R-linear map T_A completely, as a module homomorphism from a free module is determined by what it does to the standard basis elements. We show that T defines a ring homomorphism:

(1) *T sends the multiplicative identity to the multiplicative identity.* The identity of $M_{k\times k}$ is the identity matrix I, whose entries consist of 1 along the diagonal and 0 elsewhere. Then T_I sends e_i to $\sum A_{ji} e_j = e_i$, so T_I acts as the identity on the standard basis elements. For any other element $v = \sum a_j e_j$ then, $T_I(v) = T_I(\sum a_j e_j) = \sum a_j T_I(e_j) = \sum a_j e_j = v$. So T_I is indeed the identity homomorphism from $R^{\oplus k}$ to itself.

(2) $T(A+B) = T_A + T_B$. The matrix $A+B$ has (i,j)th entry given by $A_{ij} + B_{ij}$. Then $T_{A+B}(e_i) = \sum (A+B)_{ji} e_j = \sum (A_{ji} + B_{ji}) e_j = \sum A_{ji} e_j + \sum B_{ji} e_j = T_A(e_i) + T_B(e_i)$. It follows that for an arbitrary vector v, $T_{A+B}(v) = T_A(v) + T_B(v)$.

(3) $T_{AB} = T_A \circ T_B$. Note that the (j,i)th entry of the matrix AB is given by $(AB)_{ji} = \sum_l A_{jl} B_{li}$. Then $T_{AB}(e_i) = \sum_j (\sum_l A_{jl} B_{li}) e_j = \sum_l \sum_j A_{jl} B_{li} e_j = \sum_l T_A(B_{li} e_l) = T_A(\sum_l B_{li} e_l) = T_A(T_B(e_i))$. Since $T_{AB}(e_i) = T_A \circ T_B(e_i)$ for all standard basis elements e_i, it follows that $T_{AB}(v) = T_A \circ T_B(v)$ for all elements $v \in R^{\oplus k}$, so $T_{AB} = T_A \circ T_B$.

3. Some Cayley-Hamilton applications

Let $\mathbb{F}$ be a field of characteristic p. Let A be an upper-triangular $k \times k$ matrix with entries in $\mathbb{F}$.

(a) Assume A's diagonal entries are equal to 1. Show that for the values $(3,3)$, $(5,5)$, and $(4,2)$ of (k,p), A^k is equal to $(-1)^{k-1}I$.

(b) With the hypothesis as in part (a), prove that A is an element whose order must divide k or $2k$.

(a) The determinant of $tI - A$ is given by

$$\det \begin{bmatrix} t-1 & -A_{12} & \dots & -A_{1k} \\ 0 & t-1 & \dots & -A_{2k} \\ & & & \vdots \\ 0 & 0 & \dots & \\ 0 & 0 & \dots & t-1 \end{bmatrix} = (t-1)^k.$$

By the binomial theorem, this means that the determinant of $tI - A$ is given by the polynomials

$$t^3 - 3t^2 + 3t - 1, \qquad t^4 - 4t^3 + 6t^2 - 4t + 1, \qquad t^5 - 5t^4 + 10t^3 - 10t^2 + 5t - 1$$

for $k = 3, 4, 5$ respectively. If F is a field of characteristic 3, the first polynomial is $t^3 - 1$, so by Cayley-Hamilton, $A^3 = I$. If F is a field of characteristic 2, the second polynomial is $t^4 + 1$, so by Cayley-Hamilton, $A^4 = -I$. In characteristic 5, the last polynomial is $t^5 - 1$, so by Cayley-Hamilton, $t^5 = I$.

(b) If $A^k = (-1)^{k-1}I$, if k is odd, clearly $A^k = I$, so the order of A as an element of $GL_k(F)$ must divide k. Likewise, if k is even, then $A^{2k} = (-I)^2 = I$, so the order of A must divide $2k$.

4. More Cayley-Hamilton

Let F be a field and A an $k \times k$ matrix with entries in F. When you want to compute $f(A)$ where $f(t)$ is some high-degree polynomial in t, note that by the division algorithm for polynomials, we can write

$$f(t) = q(t)\Delta(t) + r(t)$$

where $\Delta(t)$ is the characteristic polynomial of A. Then we have

$$f(A) = q(A)\Delta(A) + r(A) = r(A)$$

since $\Delta(A) = 0$ by the Cayley-Hamilton theorem. This reduces a potential costly calculation into two steps: A division of polynomials (to find r) and then a degree $k-1$ computation given by evaluating $r(A)$.

(a) If A is a 2×2 matrix which is not invertible in F, prove that A^2 is always a scalar multiple of A. Moreover, prove that A^2 is obtained from A by scaling via the trace of A.

(b) Let A be a 3×3 matrix which is not invertible, and which has trace zero. Compute A^{1000} in terms of A^2 and the degree 1 coefficient of $\Delta(t)$. Derive a general formula for A^N in terms of A^2 and the degree 2 coefficient of $\Delta(t)$.

(c) Let

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 0 & -1 \\ 5 & 2 & -1 \end{bmatrix}.$$

Compute A^{2014} using the methods above.

(d) What is A^{2014} if you consider A as a matrix with entries in $\mathbb{F} = \mathbb{Z}/2\mathbb{Z}$?

(a) If A is not invertible in a field F, then its determinant must be zero. (Recall a matrix is invertible in a ring if and only if its determinant is a unit int he ring.) Since the constant term of the characteristic polynomial of A is the determinant, Cayley-Hamilton tells us A must satisfy the equation

$$A^2 + aA = 0$$

where $t^2 + at$ is the characteristic polynomial of A. Hence $A^2 = -aA$, and A^2 is some scalar multiple of A.

(b) By before, the determinant of A is $(-1)^{k-1}$ times the constant term of the characteristic polynomial, while the trace is -1 times the degree $(k-1)$ term fo the characteristic polynomial. So if both of these is zero, the characteristic polynomial of A is of the form $t^3 - at$ for some number $a \in F$. So let us divide the polynomial t^{1000} by this polynomial and find the remainder. We find that

$$t^{1000} = (t^3 - at)q(t) + r(t)$$

where $q(t) = t^{997} + at^{995} + a^2t^{993} + a^3t^{991} + \ldots + a^{498}t$, or

$$q(t) = \sum a^i t^{1000-3-2i},$$

and $r(t) = a^{499}t^2$. Let us evaluate this polynomial on A:

$$A^{1000} = (A^3 - aA)q(A) + r(A).$$

Sine $A^3 - aA$ is the chracteristic polynomial of A, by Cayley-Hamilton, it evaluates to zero. Hence

$$A^{1000} = r(A) = a^{499}A^2$$

where a is the degree 1 coefficient of the characteristic polynomial. More generally, if we divide the polynomial t^N by the characteristic polynomial, we have that

$$q(t) = \sum a^i t^{N-3-2i}$$

so if i is the largest integer for which $N - 3 - 2i > 0$,

$$A^N = r(A) = a^{i+1}t^{N-3-2i+1}.$$

Note that $N - 3 - 2i + 1$ must be equal to 1 or to 2.

(c) Let us compute the characteristic polynomial of A:

$$\det(tI - A) = \det \begin{bmatrix} t-1 & -2 & -3 \\ -1 & t & 1 \\ -5 & -2 & t+1 \end{bmatrix}$$

which equals

$$(t-1)[t^2 + t + 2] + 2(-t - 1 + 5) - 3(2 + 5t) = t^3 - 16t.$$

Now, $2014 - 3 = 2011$, so the value of i from the previous problem is 1005. So by the above work, we know that A^{2014} must equal

$$A^{2014} = 16^{1006}A^2.$$

(d) If F has characteristic 2, $16x = 0$ for any $x \in F$, so the entries of the matrix $16^{1006}A^2$ are all zero. So $A^{2014} = 0$.

Rings and ideals

5. Basics of rings

(a) Give an example of a non-commutative ring with a zero divisor. (Make sure to identify the zero divisor.)
(b) Given an example of a commutative ring with a zero divisor.

(a) Consider the ring of 2 by 2 matrices with real entries. Then the elements
$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, B = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$
satisfy
$$AB = 0.$$
Hence both B and A are zero divisors in this ring. (Indeed, we can consider A and B as matrices with coefficients in any ring R with $1 \neq 0$, and these would be examples of zero divisors in the ring $M_{2\times 2}(R)$.) Note that although $AB = 0$, $BA = A \neq 0$.
(b) Consider the ring $\mathbb{Z}/6\mathbb{Z}$. Then $\overline{2} \cdot \overline{3} = \overline{6} = 0$. Or, if you consider the ring $\mathbb{R}[t]/(t^2)$, we have that $\overline{t} \cdot \overline{t} = \overline{t}^2 = 0$.

6. Prime ideals

Let R be a commutative ring. An ideal I is called *prime* if whenever $xy \in I$, we have that either $x \in I$ or $y \in I$.

(a) Let $f \in R$ be an irreducible element and R a PID. Show that the ideal generated by f is prime.

(b) Recall that a commutative ring is called a *domain* if it has no zero divisors. Show that if I is a prime ideal of R, then R/I is a domain.

(a) Let $xy \in (f)$. This means that $xy = af$ for some $a \in R$. Since R is a PID, every element allows for unique factorization by irreducibles. That means that $x = \prod q_i$ for some irreducibles q_i, possibly repeated, and $y = \prod p_i$. Then $xy = \prod q_i \prod p_i$ is a factorization of xy by primes. At the same time, since $a \in R$, a also has a prime factoriation $a = \prod r_i$ where each r_i is some irreducible element. Note that $af = f \prod r_i$ is a prime factorization for af, and hence for xy. By uniqueness of prime factorization, f—or a unit multiple of it—must show up in the product $\prod q_i \prod p_i$. This means $f = u'p_i$ or $u'q_i$ for some i and some unit u'. Without loss of generality assume $f = u'p_i$. Then f divides x, hence $x \in (f)$.

(b) By definition, $\overline{f} = 0 \in R/I$ if and only if $f \in I$. Well, for $\overline{x}, \overline{y} \in R/I$, we have that $xy \in I \implies x \in I$ or $y \in I$. Hence if $\overline{x} \cdot \overline{y} = 0$, we have that $\overline{x} = 0$ or $\overline{y} = 0$.

7. Prime ideals and maximal ideals

Let R be a commutative ring.

(a) Show that every maximal ideal in R is a prime ideal.
(b) Show that if R is a PID, then every non-zero prime ideal is maximal.

(a) Let $I \subset R$ be a maximal ideal. Let $xy \in I$. If x is not in I, let (I, x) be the smallest ideal containing I and x. (This is the image of the R-module homomorphism $I \oplus R \to R$ sending $(f, 1) \mapsto f + x$ for $f \in I$.) This must be equal to R since $I \subset (I, x) \subset R$ and I is maximal. Hence it contains $1 \in R$. This means

$$1 = f + gx$$

for some $f \in I, g \in R$. But then $y = fy + gxy$ by multiplying both sides by y on the right. So the righthand side is a sum of two elements in I. That is, $y \in I$.

(b) Suppose I is a prime ideal in a PID R. Then $I = (f)$ for some $f \in R$ since R is a PID. We assume $f \neq 0$ since we can assume $I \neq \{0\}$. If $xy \in I$, then either x or y is divisible by f by definition of prime ideal. Now, if we have an ideal $I \subset J \subset R$, then $J = (z)$ by definition of PID, and $I \subset J \implies f = az$ for some $a \in R$. By the previous discussion, either a or z is divisible by f. If z is, then $(z) \subset (f)$, so $J = I$. If a is, then $f = a'fz \implies 0 = f - a'fz = (1 - a'z)f$. If $I \neq \{0\}$, then since R is a domain, $a'z = 1$, so z is a unit, meaning $J = R$. Thus $I \subset J \subset R \implies J = I$ or $J = R$ whenever I is a prime ideal. That is, in a PID, every prime ideal I is maximal.

8. A ring that is not a PID

(a) Let F be a field, and let $R = F[x_1, x_2]$ be the ring of polynomials with two variables. Exhibit an ideal in R that is not principal.
(b) Show that $\mathbb{Z}[x]$—the ring of polynomials with $\mathbb{Z}$ coefficients—is not a principal ideal domain.

(a) Let $I = (x_1, x_2)$ be the ideal generated by the polynomial x_1, and by the polynomial x_2. So this is the set of all polynomials that have no constant terms. If there is some polynomial f such that $af = x_1$ for $a \in R$, we must have that f is constant, or is equal to some multiple of x_1. Likewise, if there is some polynomial f such that $bf = x_2$, we must have that f is constant, or is equal to some constant multiple of x_2. If a single polynomial f generates both x_1 and x_2, f must therefore be a constant polynomial (non-zero by assumption). But since f would then be a unit, $(f) = R$, so the only principal ideal containing (x_1, x_2) is R itself. That is, I cannot be a principal ideal.
(b) Let $R = \mathbb{Z}[x]$. Consider the ideal I generated by $2 \in \mathbb{Z}$ and by the polynomial $x \in \mathbb{Z}[x]$. This is the image of the homomorphism $R \oplus R \to R$ where $(a, b) \mapsto 2a + bx$. Let (f) be a principal ideal containing I—then there must exist $p \in R$ such that $pf = 2$, and $q \in R$ such that $qf = x$. That $pf = 2$ means f must equal ± 1 or ± 2. That $qf = x$ means that f must equal ± 1 or $\pm x$. This means $f = \pm 1$, so f is a unit in R, and we have that $(f) = R$. So the only principal ideal containing I is R itself, and I is not a principal ideal.

Modules

9. $\mathbb{Z}$-modules

(a) Show that a $\mathbb{Z}$-module is the same thing as an abelian group.
(b) Show that a map of $\mathbb{Z}$-modules (i.e., a $\mathbb{Z}$-linear homomorphism between $\mathbb{Z}$-modules) is the same thing as a homomorphism of abelian groups.

(a) Let M be an abelian group. To give M the structure of a $\mathbb{Z}$-module, we must exhibit a map

$$\mathbb{Z} \times M \to M$$

such that $(a+b)x = ax+bx$, $1x = x$ (where 1 is the multiplicative unit of $\mathbb{Z}$) and $(ab)x = a(bx)$ for all $a, b \in \mathbb{Z}, x \in M$. Well, every element of $\mathbb{Z}$ can be expressed as $a = 1 + \ldots + 1$, or as $a = -1 + \ldots + -1$ where the summation runs $|a|$ times. Hence

$$ax = (1+\ldots+1)x = x+\ldots+x \qquad (a \geq 0), \qquad ax = -(1+\ldots+-1)x = -x+\ldots+-x \qquad (a \leq 0)$$

so the map $\mathbb{Z} \times M \to M$ is completely determined by the abelian group structure of M. In other words, for any set M, the collection of abelian group structures on M is in bijection with the collection of $\mathbb{Z}$-module structure on M.

(b) Let M and N be $\mathbb{Z}$-modules. Note that the set $\mathcal{F}$ of $\mathbb{Z}$-module homomorphisms from M to N has a function to the set $\mathcal{H}$ of abelian group homomorphisms $M \to N$, since every R-module homomorphism is by definition an abelian group homomorphism (together with an additional property). We show that this function is a bijection. It is obviously an injection. It is also a surjection: A $\mathbb{Z}$-module homomorphism $f : M \to N$ is an abelian group homomorphism such that $f(ax) = af(x)$. Well, since any $a \in \mathbb{Z}$ can be expressed as a sum of 1 (as above), we have that

$$f(ax) = f(x + \ldots + x) = f(x) + \ldots + f(x) = af(x)$$

where the middle equality follows from the fact that f is a group homomorphism. So any abelian group homomorphism is automatically a $\mathbb{Z}$-module homomorphism.

10. $\mathbb{Z}[t]$-modules

Show that a $\mathbb{Z}[t]$-module structure on an abelian group M is the same thing as giving an abelian group homomorphism from M to itself.

Let $\mathcal{I}$ be the set of all ring homomorphisms from $\mathbb{Z}[t]$ to the set $\mathrm{End}(M)$ of endomorphisms of M to itself. By previous homework, we know this is in bijection with the set of all $\mathbb{Z}[t]$-module structures on M. So we will show that the set of ring homomorphisms from $\mathbb{Z}[t]$ to any target ring S is in bijection with elements of S. This shows that the set of module structures on M is in bijection with elements of $\mathrm{End}(M)$. Well, if $f : \mathbb{Z}[t] \to S$ is a ring homomorphism, we have an element $f(t) \in S$. On the other hand, since f is a ring homomorphism, and $f(1) = 1_S$, the value of $f(t)$ determines the value of f on every element of $\mathbb{Z}[t]$:

$$\begin{aligned} f(a_0 + a_1 t + \ldots a_k t^k) &= f(a_0) + f(a_1 t) + \ldots + f(a_k t^k) \\ &= f(1 + \ldots + 1) + f((1 + \ldots + 1) \cdot t) + \ldots + f((1 + \ldots + 1) \cdot t \cdot \ldots \cdot t) \\ &= (f(1) + \ldots + f(1)) + (f(t) + \ldots + f(t)) + (f(t)^k + \ldots + f(t)^k) \end{aligned}$$

where the summations happen $a_0, a_1, \ldots, a_k$ times, and if a_i is negative, we mean the summation $-1 + \ldots + -1$ with $|a_i|$ many terms. Thus, if $f(t) = f'(t)$, then $f = f'$, so this assignment is an injection. On the other hand, an arbitrary choice of element $s \in S$ determines a ring homomorphism f by assigning $f(t) = s$, and extending by the equation above. So the assignment $f \mapsto f(t)$ is a surjection as well.

11. Submodules

Let M be a left R-module. Recall that an R-*submodule* of M is a subgroup $N \subset M$ such that $rx \in N$ for all $r \in R, x \in N$.

(a) Show that the intersection of two submodules is a submodule.
(b) If R is a commutative ring and $R = M$, show that a submodule of M is the same thing as an ideal of R.

(a) The intersection of two subgroups is a subgroup. On the other hand, if $x \in N \cap N'$, then $rx \in N$ and $rx \in N'$ if N, N' are submodules. Hence $rx \in N \cap N'$.
(b) By definition, an ideal I of a commutative ring R is a subgroup of R for which $x \in I \implies rx \in I$ for all $r \in R$. Well, every ring R is a module over itself, with an R-module structure given by the function

$$R \times R \to R, \qquad (x, y) \mapsto xy$$

and by associativity and distributivity, this turns R into a left module over itself.

12. Not all modules are free

Give an example of a ring R and a left module M such that M is not isomorphic to a free R-module.

Let $R = \mathbb{Z}$ and $M = \mathbb{Z}/n\mathbb{Z}$ for $|n| \geq 2$. Then $\mathbb{Z}/n\mathbb{Z}$ has $|n| \geq 2$ elements, while $R^{\oplus k}$ has either infinitely elements, or 1 element (if $k = 0$). Hence the two sets cannot be in bijection, let alone admit a module isomorphism between them.

Computations

13. Computations with matrices

Consider the matrices

$$\begin{bmatrix} 1 & 4 \\ 5 & 7 \end{bmatrix}, \qquad \begin{bmatrix} 1 & 3 \\ 7 & 9 \end{bmatrix}, \qquad \begin{bmatrix} 2 & 4 \\ 6 & 8 \end{bmatrix}.$$

(a) Which of them are invertible as elements of $M_{2\times 2}(\mathbb{Z})$?
(b) Which are invertible as elements of $M_{2\times 2}(\mathbb{Z}/2\mathbb{Z})$?
(c) Which are invertible as elements of $M_{2\times 2}(\mathbb{Z}/7\mathbb{Z})$?

(a) Compute the determinants of each matrix. If they are equal to $\pm 1 \in \mathbb{Z}$, then the determinants are units in the ring $\mathbb{Z}$, hence the matrices are invertible in $\mathbb{Z}$.
(b) Now take the determinants of each matrix and reduce modulo 2. This is non-zero if and only if the matrix is invertible.
(c) Likewise, reduce the integer determinants modulo 7. This is non-zero if and only if the matrix is invertible.

14. Polynomial roots

Consider the polynomials

$$t^3 + 2t + 1, \qquad t^4 + 1, \qquad t^2 + 3.$$

(a) Which of these are irreducible elements of $\mathbb{Z}/2\mathbb{Z}[t]$?
(b) Which of these are irreducible elements of $\mathbb{Z}/3\mathbb{Z}[t]$?
(c) Which of these are irreducible elements of $\mathbb{Z}/5\mathbb{Z}[t]$?

For degree 3 and degree 2 polynomials, any factorization into non-units must have some factor of a linear polynomial, so irreducibility is equivalent to the absence of a root. So I'll leave those polynomials to you. But the fourth-degree polynomial is less trivial, since non-existence of a root doesn't guarantee irreducibility. For $p = 2, 5$, note that -1 admits a square root, since $1^2 = 1 = -1$ modulo 2, while $2^2 = 4 = -1$ modulo 5. So the polynomial $t^4 + 1 = (t^2 + 1)(t^2 + 1)$ modulo 2, and $t^4 + 1 = (t^2 - 2)(t^2 + 2)$ modulo 5. For $p = 3$, the process is more complicated—the only obvious strategy we have at our disposal in this class is to test by brute force whether the polynomial can be factored by degree 2 polynomials.

Classification of finitely generated PIDs

15. Statement

State the classification of finitely generated modules over a PID.

Let R be a principal ideal domain (PID). Suppose that M is a finitely generated R-module.[1] Then M is isomorphic to the module

$$R^{\oplus n_0} \oplus R/(p_1^{n_1}) \oplus \ldots \oplus R/(p_l^{n_l})$$

where $n_0 \geq 0$, $n_i \geq 1$, and $l \geq 0$ are integers, and each p_i is an irreducible element of R. If M is isomorphic to another module of the form

$$R^{\oplus m_0} \oplus R/(q_1^{m_1}) \oplus \ldots \oplus R/(q_k^{m_k})$$

where each q_i is an irreducible element, and $m_0 \geq 0, m_i \geq 1$, $k \geq 0$, then $k = l, m_0 = n_0$, and there is some re-ordering of indices so that q_i is a unit multiple of p_i and $n_i = m_i$ for all i. [2]

[1] This means that for some $k \geq 0$, M admits some homomorphism of R-modules, $R^{\oplus k} \to M$ which is a surjection.

[2] Of course, $R^{\oplus n_0}$ is given the usual R-module structure as a free R-module, while $R/(p_i^{n_i})$ is given the quotient module structure:

$$R \times R/(p_i^{n_i}) \to R/(p_i^{n_i}), \qquad (f, \overline{g}) \mapsto \overline{fg}.$$

16. Classifying abelian groups

(a) How does the theorem let us classify finitely generated abelian groups?
(b) Classify all abelian groups of order 12.
(c) Classify all abelian groups of order 16.

(a) Take $R = \mathbb{Z}$. This is a PID since every ideal of $\mathbb{Z}$ is equal to an ideal of the form $(n) = n\mathbb{Z}$ for $n \in \mathbb{Z}$. The irreducible elements of $\mathbb{Z}$ are those numbers $\pm p$ where p is a prime. Finally, any $\mathbb{Z}$-module is nothing more than an abelian group, so we can conclude that any finitely generated abelian group is isomorphic to an abelian group of the form

$$\mathbb{Z}^{\oplus n_0} \oplus \mathbb{Z}/(p_1^{n_1}) \oplus \ldots \oplus \mathbb{Z}/(p_l^{n_l}).$$

(b) The prime factorization of 12 is $3 \cdot 2 \cdot 2$. Because the size of the abelian group M must be 12, and the size of an abelian group as above is given by

$$p_1^{n_1} \cdot \ldots \cdot p_l^{n_l}$$

we see that the possible choices of p_i, n_i are as follows:

$$p_1 = 2, p_2 = 1, p_3 = 1, n_i = 1, \qquad p_1 = 2, p_3 = 1, n_1 = 2, n_2 = 1.$$

So M must be isomorphic to

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \qquad \text{or} \qquad \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}.$$

(c) Likewise, the possible choices for p_i and n_i are

$$p_1 = p_2 = p_3 = p_4 = 2, n_1 = n_2 = n_3 = n_4 = 1, \qquad p_1 = p_2 = p_3 = 2, n_1 = n_2 = 1, n_3 = 2,$$
$$p_1 = p_2 = 2, n_1 = n_2 = 2, \qquad p_1 = p_2 = 2, n_1 = 1, n_2 = 3, \qquad p_1 = 2, n_1 = 4.$$

So we have the possible groups

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, \qquad \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$$
$$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}, \qquad \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}, \qquad \mathbb{Z}/16\mathbb{Z}.$$

17. Another way to phrase classification of abelian groups

(a) Let k, m, n be integers. Prove that $\mathbb{Z}/k\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ if and only if $k = mn$ and m, n are relatively prime.

(b) Assume the classification of finitely generated abelian groups stated in class. Prove: If A is a finitely generated abelian group, it is isomorphic to a group of the form

$$\mathbb{Z}/n_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/n_k\mathbb{Z}$$

where n_i divides n_{i+1} for all $1 \leq i \leq k-1$.

(a) Let $(1, 1) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Since the order of this group is mn, we know that the order of $(1, 1)$ must divide mn. On the other hand,

$$(1, 1) + \ldots + (1, 1) = (\overline{a}, \overline{a})$$

where the summation happens a times. For the first coordinate to equal zero, $\overline{a} = 0$ modulo m, and for the left coordinate to equal zero, we must have that a is a multiple of n. That is, a must be a multiple of both m and n. But since m and n are relatively prime, the smallest multiple of both m and n is mn itself. On the other hand, the order of any element must divide the order of the group containing it so we have that $a|mn$ and $mn \leq a$. This means $a = mn$, so $(1, 1)$ generates the whole group. On the other hand, suppose that $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/k\mathbb{Z}$. Then we must have that $k = mn$ since isomorphic groups have the same order. If m, n are not relatively prime, then let $a = lcm(m, n) < mn$. Then any element $(x, y) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ would have order dividing a[3]and in particular, order strictly less than mn. So $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ could not have any element of order mn, and in particular, cannot be cyclic.

[3]For $(x, y) + \ldots + (x, y) = (ax, ay)$. Since $a = bm$, $ax = b(mx) = 0 \in \mathbb{Z}/m\mathbb{Z}$. Likewise, since $a = nc, ay = 0 \in \mathbb{Z}/n\mathbb{Z}$. So (1,1) must have order dividing a.

Groups

18. Your common mistakes

(a) Give an example of a group G, and an abelian subgroup $H \subset G$, such that H is not normal in G.

(b) Given an example of a group G, and a sequence of subgroups

$$G_1 \subset G_2 \subset G$$

such that $G_1 \triangleleft G_2$ and $G_2 \triangleleft G$, but G_1 is not normal in G.

(a) Let $H \subset S_3$ be the subgroup generated by the 2-cycle (12). This is not normal, since (12) is conjugate to (13) but $(13) \notin H$. On the other hand, it is clearly abelian, since it's cyclic.

(b) Let $G = S_4$ and $G_2 = V$ be the group of order 4 in S_4 isomorphic to the Klein 4-group. V has elements

$$1, (12)(34), (13)(24), (23)(14).$$

Note that since V is abelian, any subgroup of it is normal in V—in particular, let G_1 be the subgroup generated by $(12)(34)$. Then $G_1 \triangleleft G_2$. And $G_2 \triangleleft G$ since every element of S_4 with cycle shape given by two disjoint 2-cycles is in V, while every element of V is of this cycle shape. We know that the group generated by $(12)(34)$ is not normal in S_4 itself—for instance, $(12)(34)$ is conjugate to $(13)(24)$, but the latter is not in the subgroup generated by the former.

19. Sylow's Theorems

Let n_p denote the number of Sylow p-subgroups of G.

(a) * Let $G = S_4$. Compute n_2.
(b) Let $G = S_4$. Compute n_3.
(c) Let $G = D_{2p}$, the dihedral group with $2p$ elements, where $p > 2$ is a prime. Compute n_2 and n_p.

(a) Since $|G| = 24 = 8 \cdot 3$, the Sylow theorems tell us that n_2 divides 3, and is equal to 1 modulo 2. Thus n_2 is equal to 3 or to 1. You can exhibit a subgroup of order 8, and show it is not a normal subgroup. Thus n_2 must equal 3.

(b) n_3 must divide 8, and be equal to 1 modulo 3. The only such numbers are 1 or 4. Well, there is an obvious subgroup of order 3 given by the group generated by (123). This group cannot be normal because it does not contain all elements with the same cycle shape—for instance, it does not contain (124). Hence n_3 must be 4. (Recall that, by the Sylow theorems, $n_p = 1$ if and only if there is only one Sylow p-subgroup.)

(c) n_p has to equal 1 because it must divide 2, and equal 1 modulo p. To compute n_2, note that n_2 must equal 1 modulo 2, while it must also divide p. So we show that $n_2 \neq 1$. Note that the element $g \in D_{2p}$ given by reflection is an element of order 2, so it generates a group of order 2. Note that if you conjugate g by a rotation of $2\pi/p$, you do not get back g. Hence $n_2 \neq 1$.

20. Actions and orbit-stabilizer

(a) Show that $H \triangleleft G$ if and only if the normalizer of H is all of G.
(b) Let G be a finite group, and $H \subset G$ a subgroup. Show that the number of subgroups of G conjugate to H is equal to the size of G, divided by the order of the normalizer of H.
(c) Let $x \in G$ be an element, with $|G|$ finite. Show that the number of elements conjugate to x is equal to the size of G, divided by the number of elements that commute with x.

(a) Definition of normalizer.
(b) Orbit-stabilizer theorem; G acts by conjugation on the set of all subgroups of G. The stabilizer of a subgroup is the normalizer, and the orbit of H is the set of all subgroups conjugate to H.
(c) G acts on itself by conjugation. The elements that fix x are those that commute with x. The orbit of x is the set of all elements conjugate to x.

21. Prove Lagrange's Theorem

Prove Lagrange's Theorem.

Let $H \subset G$ be a subgroup of a finite group G. Lagrange's Theorem says that $|H|$ must divide $|G|$. Note that H acts on G via multiplication:

$$H \times G \to G, \qquad (h, g) \mapsto hg.$$

Then G is a disjoint union of the orbits of the H-action:

$$G = \coprod_{orbits} \mathcal{O}$$

Claim: For each orbit, $|\mathcal{O}| = |H|$. If we have this claim, we see that

$$|G| = |H| + \ldots + |H|$$

so $|H|$ divides $|G|$. To prove this claim, note that the orbit of $1_G \in G$ is

$$\{h1_G \in G \text{ s.t. } h \in H\} = \{h \in G \text{ s.t. } h \in H\} = H$$

so the orbit of 1_G *is the set* H, meaning $|\mathcal{O}_{1_G}| = |H|$. On the other hand, if $\mathcal{O}_g$ is another orbit, we have a bijection $\mathcal{O}_1 \to \mathcal{O}_g$ by sending

$$x \mapsto xg \in \mathcal{O}_g, \qquad x \in \mathcal{O}_{1_G}.$$

This is a bijection because it has an inverse given by sending $hg \in \mathcal{O}_g$ to $hgg^{-1} \in \mathcal{O}_{1_G}$. Hence every orbit is in bijection with $\mathcal{O}_{1_G}$, meaning $|\mathcal{O}| = |H|$ for every orbit.

22. Cayley's Theorem

(a) Show that every group acts on itself.
(b) Show that every finite group is isomorphic to a subgroup of S_n for some n. This is called Cayley's Theorem.

(a) There are two equivalent ways to exhibit a group action of G on a set X. By exhibiting a group homomorphism

$$\phi : G \to \text{Aut}_{Set}(X)$$

or a function

$$G \times X \to X, \qquad (g, x) \mapsto gx$$

satisfying
 (a) $1_G x = x$ for all $x \in X$,
 (b) $g(hx) = (gh)x$ for all $g, h \in G$ and $x \in X$.

A group G acts on itself by the function

$$G \times G \to G, \qquad (g, x) \mapsto gx$$

where gx is the group multiplication. (a) follows from the definition of identity, and (b) follows from associativity of G's multiplication.

(b) Since we have a group action, we have a group homomorphism $\phi : G \to \text{Aut}_{Set}(X)$. If we show this is an injection, by the first isomorphism theorem, we have the group isomorphisms

$$G \cong G/\{1_G\} \cong \text{image}(\phi) \subset \text{Aut}_{Set}(X) \cong S_{|X|}.$$

This last group is the symmetric group on $|X|$ elements. To show ϕ is an injection, we must show that it has trivial kernel—that is, that $\phi_g = \text{id}$ implies that $g = 1_G$. But this follows from the uniqueness of the identity element of a group.

23. Groups of order 8

Recall the quaternion ring, otherwise called the Hamiltonians. Consider the set

$$Q = \{\pm 1, \pm i, \pm j, \pm k\} \subset \mathbb{R}^4$$

where

$$1 = (1,0,0,0) \qquad i = (0,1,0,0) \qquad j = (0,0,1,0) \qquad k = (0,0,0,1).$$

(a) Show that Q is a group of order 8.
(b) Show that Q is non-abelian.
(c) Write down all subgroups of Q.
(d) * Show that Q is not isomorphic to $D_{2\cdot 4} = D_8$, the dihedral group with 8 elements.

(a) Claim: Let R be a ring, and let $R^\times$ be the subset of all elements in R with a multiplicative inverse. (I.e., the set of units of R.) Then $R^\times$ is a group. Proof of claim: Since 1_R is a unit, with inverse itself, $R^\times$ has an identity by definition of 1_R. Multiplication is associative since multiplication in R is associative, and every element admits an inverse by definition of units for a ring. Now that the claim is proven, denote the quaternions by $\mathbb{H}$. Recall that the quaternions are a ring, and that every non-zero element of the ring admits a multiplicative inverse. (This was a homework problem.) Then it follows that $\mathbb{H} - \{0\}$ is a group (non-abelian, since $\mathbb{H}$'s multiplication is not commutative), with identity given by the multiplicative identity $(1,0,0,0)$ of $\mathbb{H}$. We must show that $Q \subset \mathbb{H} - \{0\}$ is a subgroup. In any ring, we have that $(-a)\cdot b = -(a \cdot b) = a \cdot (-b)$, so to show closure, it suffices to show that

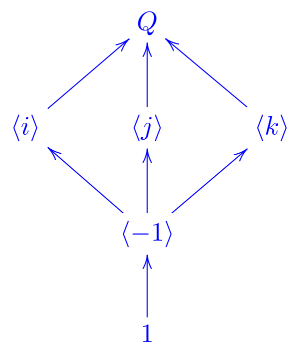
$$i \cdot j = k, \qquad i \cdot k = -j, \qquad j \cdot k = i$$

which you can check. Moreover, can see that for any $g \in Q$, $g\cdot(-g) = 1$, so every element has an inverse. Since $Q \subset \mathbb{H} - \{0\}$ is a subgroup, it is in particular a group. To check it has order 8, we simply count the elements—there are 8 of them.
(b) $ij = k$ while $ji = -k$.
(c) Tedious, but we can do this systematically as follows.
   (a) We have the subgroups generated by each element. So for instance,

$$\langle i \rangle = \{1, i, -1, -i\}$$

   is a subgroup of order 4, as are $\langle j \rangle$ and $\langle k \rangle$. These subgroups contain a unique subgroup of order 2, the one generated by -1. Note that $\langle -j \rangle = \langle j \rangle$.

(b) Now suppose that a subgroup contains both i and j. Then it contains $-1 = i^2, -i = i^3$, $k = ij$, and $-k = ji$. That is, the whole group. So we have that the subgroups of Q are given by



where the arrows indicate inclusions. Note that each of $\langle i\rangle, \langle j\rangle, \langle k\rangle$ are each subgroups of order 4, hence subgroups of index 2, hence normal.

(c) As a side note, observe that $\langle -1\rangle = \{1, -1\}$ is the center of this group. As a result, $\langle -1\rangle$ is normal in Q. It is the unique subgroup of order 2 in Q.

(d)

24. Some big theorems

(a) Let p be a prime number. If $n \in \mathbb{Z}$ is not divisible by p, prove that

$$n^{p-1} - 1$$

is divisible by p. This is called Fermat's Little Theorem. (Hint: If $\mathbb{Z}/p\mathbb{Z}$ is a field, what can you say about $\mathbb{Z}/p\mathbb{Z} - \{0\}$?)

(b) Show that every finite group is isomorphic to a subgroup of S_n for some n. This is called Cayley's Theorem. (Hint: Every group acts on itself by left multiplication.)

(a) If p is a prime, $\mathbb{Z}/p\mathbb{Z}$ is a field. So $\mathbb{Z}/p\mathbb{Z} - \{0\}$ is a group. Let $\overline{n}$ be an element. Since $\mathbb{Z}/p\mathbb{Z} - \{0\}$ has order $p-1$, the order of $\overline{n}$ must divide $p-1$. Which is to say,

$$\overline{n}^{p-1} = \overline{1}$$

where $\overline{1}$ is the multiplicative unit of $\mathbb{Z}?p\mathbb{Z}$. So we have that for any $\overline{n} \in \mathbb{Z}/p\mathbb{Z} - \{0\}$,

$$\overline{n}^{p-1} - \overline{1} = \overline{0} \in \mathbb{Z}/[\mathbb{Z}$$

So for any number n not divisible by p,

$$n^{p-1} - 1$$

equals zero modulo p—i.e., is divisible by p.

(b) We did this in a previous problem on this practice set.