Worksheets

Here are two sets of problems, to be done during April 15–April 29 (approximately).

The first set of problems isn't like anything we've done before, but should feel familiar; they involve working with the complex numbers as a two-dimensional vector space over $\mathbb{R}$.

The second set of problems is a special case of the investigation of *algebraic numbers* we did in class. It's a little more abstract, but more closely parallels what we did in class.

There are connections and correspondences between the two sets, and you're welcome to do them in whatever order you like.

At the end of this you'll find lecture notes on algebraic numbers and linear algebra.

Please don't hesitate to email if you have any questions.

Professor Jeff Achter
Colorado State University

M469 Linear Algebra II
Spring 2009

In these problems, think of $\mathbb{C}$ as a 2-dimensional vector space over $\mathbb{R}$, with basis $\{1, i\}$.

If $\beta \in \mathbb{C}$, write $\beta = a + bi$, with $a, b \in \mathbb{R}$. (Note that these are the coordinates of β with respect to our choice of basis!)

The complex conjugate of β is $\overline{\beta} = a - bi$. Let $\kappa : \mathbb{C} \to \mathbb{C}$ be the complex conjugation map $\kappa(\beta) = \overline{\beta}$. This is a $\mathbb{R}$-linear transformation of $\mathbb{C}$; $\kappa \in \mathcal{L}(\mathbb{C})$.

Recall that $|\beta|^2 = \beta\overline{\beta}$.

If you get stuck on these problems, try working them out in the explicit cases $\beta = 2$, $\beta = 3 + 4i$.

1. (a) Compute the matrix $[\kappa]$.
   (b) Describe two subspaces $U, V \subset \mathbb{C}$ such that
      i. U and V are one-dimensional subspaces;
      ii. U and V are κ-invariant;
      iii. $U \cap V = \{0\}$.
      (Then $\mathbb{C} = U \oplus V$.)

2. Let $\beta = a + bi \in \mathbb{C}$. Then multiplication by β gives a linear transformation $T_\beta \in \mathcal{L}(\mathbb{C})$.

   (a) Compute the matrix $[\beta] = [T_\beta]$.
   (b) What is $\det(T_\beta)$? Equivalently, what is $\det([\beta])$?
   (c) Express $\det(T_\beta)$ in terms of β and $\overline{\beta}$.
   (d) Express $\det(T_\beta)$ in terms of $|\beta|$.

3. The *trace* of a matrix is the sum of its diagonal entries (see [KK] p. 87).
   In the situation of Problem 2, express the trace $\mathrm{tr}[T_\beta]$ in terms of β and $\overline{\beta}$.

4. Continue the notation of Problem 2.

   (a) Compute the characteristic polynomial $\chi_{T_\beta}(x)$.
   (b) Express $\chi_{T_\beta}(x)$ in terms of its trace and determinant.
   (c) Express $\chi_{T_\beta}(x)$ in terms of β and $\overline{\beta}$.

5. (a) Show that $\chi_{T_\beta}(\beta) = 0$.
   (b) Suppose $\beta \in \mathbb{R} \subset \mathbb{C}$. Show that $\chi_{T_\beta}(x)$ factors (as a polynomial over $\mathbb{R}$).
   (c) Suppose $\beta \notin \mathbb{R}$. Show that χ_{T_β} is irreducible, i.e., that χ_{T_β} does not factor (as a polynomial over $\mathbb{R}$).

Fix an integer D which is *not* a square. It turns out that the condition *there is no* $a \in \mathbb{Z}$ *such that* $a^2 = D$ is the same as the condition "there is no $a \in \mathbb{Q}$ such that $a^2 = D$." In this set of exercises, you are welcome to fix a value of D (say, $D = 3$) and work with it, although this won't be appreciably easier.

1. Show that the minimal polynomial of $\sqrt{D}$ is $\mu(x) = \mu_{\sqrt{D}}(x) = x^2 - D$.

   Therefore, $\mathbb{Q}[\sqrt{D}]$ is a degree two extension of $\mathbb{Q}$, with basis $\{1, \sqrt{D}\}$.

2. An element β of $\mathbb{Q}[\sqrt{D}]$ can be written as $\beta = a + b\sqrt{D}$ for some $a, b \in \mathbb{Q}$.

   (a) The numbers a and b are uniquely determined. Why? (You don't have to prove anything here, just understand which result from class proves this.)

   (b) Suppose $\beta = a + b\sqrt{D}$ and $\gamma = c + d\sqrt{D}$.

      i. What is $\beta + \gamma$?

      ii. What is $\beta \cdot \gamma$?

      In each case, express your answer in the form $e + f\sqrt{D}$, $e, f \in \mathbb{Q}$.

   Unless otherwise specified, think of $\mathbb{Q}[\sqrt{D}]$ as a two-dimensional vector space over $\mathbb{Q}$. In particular, $\mathcal{L}(\mathbb{Q}[\sqrt{D}])$ means $\mathcal{L}_{\mathbb{Q}}(\mathbb{Q}[\sqrt{D}], \mathbb{Q}[\sqrt{D}])$, so that an element of $\mathcal{L}(\mathbb{Q}[\sqrt{D}])$ is represented by an element of $\mathrm{Mat}_2(\mathbb{Q})$.

3. There is a map

$$\begin{tikzcd} \mathbb{Q}[\sqrt{D}] \arrow[r, "\sigma"] & \mathbb{Q}[\sqrt{D}] \\ a + b\sqrt{D} \arrow[r, mapsto] & a - b\sqrt{D} \end{tikzcd}$$

   (a) Show that σ is a linear transformation.

   (b) Write down the matrix $[\sigma]$.

4. If $\beta \in \mathbb{Q}[\sqrt{D}]$, its trace is $\mathrm{tr}(\beta) = \beta + \sigma(\beta)$ and its norm is $\mathcal{N}(\beta) = \beta \cdot \sigma(\beta)$.

   (a) Suppose $\beta = a + b\sqrt{D}$. Write down formulas for:

      i. $\mathrm{tr}(\beta)$

      ii. $\mathcal{N}(\beta)$

   (b) Is $\beta \mapsto \mathrm{tr}(\beta)$ a linear transformation? If so, write down its matrix; if not, explain.

   (c) Is $\beta \mapsto \mathcal{N}(\beta)$ a linear transformation? If so, write down its matrix; if not, explain.

5. Let $\beta = a + b\sqrt{D} \in \mathbb{Q}[\sqrt{D}]$. Then multiplication by β gives a linear transformation $T_\beta \in \mathcal{L}(\mathbb{Q}[\sqrt{D}])$. To ease notation, write $[\beta]$ for $[T_\beta]$.

   (a) Suppose $\beta = a \in \mathbb{Q} \subset \mathbb{Q}[\sqrt{D}]$. Compute the matrix $[a]$.

(b) Compute the matrix $[\sqrt{D}]$.

(c) Suppose $\beta = a + b\sqrt{D}$. Compute $[\beta]$.

6. (a) Compute $\mathrm{tr}([\beta])$ and $\det([\beta])$. (The trace of a matrix is the sum of its diagonal entries.)

   (b) How are these related to $\mathrm{tr}(\beta)$ and $\mathcal{N}(\beta)$?

7. In this problem, we'll show that the ring $\mathbb{Q}[\sqrt{D}]$ is actually a field, by using linear algebra to show that every nonzero element has a multiplicative inverse.

   (a) Show that $\mathcal{N}(\beta) = 0$ if and only if $\beta = 0$. (HINT: *Remember, D is not a square – so,* $\frac{a^2}{b^2} = D$ *has no solutions with* $a, b \in \mathbb{Q}$*.*)

   (b) Suppose $\beta \neq 0$. Show that T_β is invertible, i.e., that the matrix $[\beta]$ has an inverse.

   (c) Suppose $\beta \neq 0$. Show there exists $\gamma \in \mathbb{Q}[\sqrt{D}]$ such that $[\gamma] \cdot [\beta] = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

   (d) For β and γ as above, show that $\gamma \cdot \beta = 1$.

8. (a) Compute the characteristic polynomial $\chi_{T_\beta}(x)$.

   (b) What is $\chi_{T_\beta}(\beta)$?

9. For this problem – *and this problem only!* – view $[\beta]$ as a matrix with coefficients in $\mathbb{C}$. What are the eigenvalues of $[\beta]$?

1 Interlude: number theory

1.1 Rings of algebraic numbers

A number $\alpha \in \mathbb{C}$ is called *algebraic* (over $\mathbb{Q}$) if it satisfies $f(\alpha) = 0$ for some polynomial $f(x) \in \mathbb{Q}[x]$.

Example $\sqrt[3]{2}$ is algebraic, since it's a root of the polynomial $x^3 - 2 = 0$.

If α is algebraic, let $\mu_\alpha(x) \in \mathbb{Q}[x]$ be the smallest nonconstant monic polynomial such that $\mu_\alpha(\alpha) = 0$. The degree of α is $\deg(\alpha) = \deg \mu_\alpha(x)$.

Example The minimal polynomial of $i = \sqrt{-1}$ is $x^2 + 1$. This is easy to verify; clearly, i doesn't satisfy a linear equation, and this is a quadratic polynomial it satisfies.

Example The minimal polynomial of $\sqrt[3]{2}$ is $x^3 - 2$. It's clear that $\sqrt[3]{2}$ is a solution to $x^3 - 2 = 0$. Grant the next lemma; then the minimal polynomial $\mu_{\sqrt[3]{2}\alpha}(x)$ divides $x^3 - 2$, and it suffices to show that there's no factorization $x^3 - 2 = (x - a)(x^2 + bx + c)$ with $a, b, c \in \mathbb{Q}$. Suppose there is such a solution; then

$$\begin{aligned} (x-a)(x^2+bx+c) &= x^3 - 2 \\ x^3 + (b-a)x^2 + (-ab+c)x - ac &= x^3 - 2 \end{aligned}$$

So equate coefficients. We have the system of (nonlinear, for once!) equations

$$\begin{aligned} b - a &= 0 \\ -ab + c &= 0 \\ -ac &= -2 \end{aligned}$$

By the first equation, $a = b$; by the second, $c = ab = a^2$; and by the third, $ac = a^3 = 2$, which is impossible if $a \in \mathbb{Q}$.

Remember that we write $f(x)|g(x)$ if $f(x)$ divides $g(x)$ (evenly), i.e., if there exists some polynomial $h(x)$ such that $f(x)h(x) = g(x)$.

Lemma Suppose α is algebraic. Suppose $f(x) \in \mathbb{Q}[x]$. Then $f(\alpha) = 0 \iff \mu_\alpha(x)|f(x)$.

Proof The proof is much like before. One direction is trivial. Conversely, suppose $f(\alpha) = 0$. Using long division with remainder for polynomials, write

$$f(x) = q(x)\mu_\alpha(x) + r(x)$$

where $\deg r(x) < \deg \mu_\alpha(x)$. Now, $f(\alpha) = 0$, so $q(\alpha)\mu_\alpha(\alpha) + r(\alpha) = 0$, so $r(\alpha) = 0$. By minimality, this forces $r = 0$. □

Example Suppose $f(x) \in \mathbb{Q}[x]$. Then $f(\sqrt[3]{2}) = 0 \iff x^3 - 2|f(x)$.

Let $\mathbb{Q}[\alpha]$ be the smallest ring which contains both $\mathbb{Q}$ and α. Note that $\mathbb{Q}[\alpha]$ must contain things like α^2, as well, and thus things like $a + b\alpha + c\alpha^2$, etc.

Lemma $\mathbb{Q}[\alpha]$ is a vector space over $\mathbb{Q}$.

Proof Just forget about the fact that we can multiply elements of $\mathbb{Q}[\alpha]$ by each other, and instead just multiply by elements of the base field, $\mathbb{Q}$. □

Remark This is quite similar to the way in which $\mathbb{C}$ is a vector space over $\mathbb{R}$, say with basis $\{1, i\}$.

Proposition Let $m = \deg\alpha$; then $\mathbb{Q}[\alpha]$ is a vector space over $\mathbb{Q}$ of dimension m.

Example $\mathbb{Q}[\sqrt[3]{2}] = \{b_0 + b_1\sqrt[3]{2} + b_2\sqrt[3]{4}\}$. For instance, suppose $\beta = 2 + 5\sqrt[3]{4}$ and $\gamma = 1 + 2\sqrt[3]{2} + 3\sqrt[3]{4}$. Then

$$\begin{aligned}
\beta\gamma &= (2 + 5\sqrt[3]{4})(1 + 2\sqrt[3]{2} + 3\sqrt[3]{4}) \\
&= 2(1 + 2\sqrt[3]{2} + 3\sqrt[3]{4}) + 5\sqrt[3]{4}(1 + 2\sqrt[3]{2} + 3\sqrt[3]{4}) \\
&= 2 + 4\sqrt[3]{2} + 6\sqrt[3]{4} + 5\sqrt[3]{4} + 10\sqrt[3]{4}\sqrt[3]{2} + 15\sqrt[3]{4}\sqrt[3]{4} \\
&= 2 + 4\sqrt[3]{2} + 6\sqrt[3]{4} + 5\sqrt[3]{4} + 10\sqrt[3]{8} + 15\sqrt[3]{16} \\
&= 2 + 4\sqrt[3]{2} + 6\sqrt[3]{4} + 5\sqrt[3]{4} + 20 + 30\sqrt[3]{2} \\
&= 22 + 34\sqrt[3]{2} + 11\sqrt[3]{4}.
\end{aligned}$$

Proof We'll prove the proposition in a few steps; briefly, we'll show that

$$\mathbb{Q}[\alpha] = R_\alpha := \{b_0 + b_1\alpha + \cdots + b_{m-1}\alpha^{m-1}\},$$

and that $\{1, \alpha, \cdots, \alpha^{m-1}\}$ is a basis for R_α as a vector space over $\mathbb{Q}$.

Lemma For all $n \in \mathbb{Z}_{\geq 0}$, $\alpha^n \in R_\alpha$.

Proof The proof is by induction on n. Let $\mu(x) = x^m + \sum_{i=0}^{m-1} a_i x^i$ be the minimal polynomial of α.

The claim is certainly true for $0 \leq n \leq m-1$. For $n = m$, since $\mu(\alpha) = 0$, we have

$$\mu(\alpha) = \alpha^m + \sum_{i=0}^{m-1} a_i\alpha^i = 0$$

$$\alpha^m = -\sum_{i=0}^{m-1} a_i\alpha^i$$

Now suppose the claim is true for $n-1$; we wish to show that α^n can be expressed as a $\mathbb{Q}$-linear combination of $1, \alpha, \cdots, \alpha^{m-1}$. By the inductive hypothesis, there are numbers $b_0, \cdots, b_{m-1} \in \mathbb{Q}$

such that $\alpha^{n-1} = \sum_{i=0}^{m-1} b_i\alpha^i$. Then

$$\begin{aligned}\alpha^n &= \alpha\alpha^{n-1}\\ &= \alpha\cdot(\sum_{i=0}^{m-1} b_i\alpha^i)\\ &= \sum_{i=0}^{m-1} b_i\alpha^{i+1}\\ &= (\sum_{i=1}^{m-1} b_{i-1}\alpha^i) - b_{m-1}\alpha^m\\ &= (\sum_{i=1}^{m-1} b_{i-1}\alpha^i) - \sum_{i=0}^{m-1} b_{m-1}a_i\alpha^i\\ &\in \operatorname{span}(1,\alpha,\cdots,\alpha^{m-1}).\end{aligned}$$

□

Lemma $R_\alpha = \mathbb{Q}[\alpha]$ is a ring.

Proof It's clear that R_α is closed under addition. To show that it is closed under multiplication, choose two elements $\beta = \sum b_i\alpha^i$ and $\gamma = \sum c_j\alpha^j$. Then

$$\begin{aligned}\beta\gamma &= (\sum b_i\alpha^i)(\sum c_i\alpha^j)\\ &= \sum_i\sum_j b_ic_j\alpha^{i+j}\end{aligned}$$

(One can be more clever about organizing this information, but it's not necessary.) Since each $\alpha^{i+j} \in R_\alpha$, so is $b_ic_j\alpha^{i+j}$, and thus so is $\beta\gamma$. □

Proof of proposition So, at this point we know that $R_\alpha = \mathbb{Q}[\alpha]$; and for tautological reasons, we know that $\{1,\alpha,\cdots,\alpha^{m-1}\}$ spans $\mathbb{Q}[\alpha]$ as a $\mathbb{Q}$-vector space. So we need to show that this set is linearly independent.

Suppose that $\sum b_i\alpha^i = 0$; then α is a root of the polynomial $f(x) = \sum b_ix^i$, whose degree is less than m; by definition, $f(x)$ is the zero polynomial, and thus each $b_i = 0$. □

1.2 Back to linear algebra

Consider $\mathbb{Q}[\alpha]$ as a vector space over $\mathbb{Q}$, with basis $\{1,\alpha,\cdots,\alpha^{m-1}\}$.

Lemma If $\beta \in \mathbb{Q}[\alpha]$, then multiplication by β is a linear transformation of $\mathbb{Q}[\alpha]$.

Proof Omitted. □

Call this linear transformation T_β, I suppose, and let $[\beta] = [T_\beta]$ with respect to this basis.

Example In $\mathbb{Q}[\sqrt[3]{2}]$, try multiplication by 5, by $\sqrt[3]{2}$, and by some random element:

- Use $\beta = 5$. Then

$$\begin{aligned}
T_5(1) &= 5 \cdot 1 = 5 \cdot 1 + 0 \cdot \sqrt[3]{2} + 0 \cdot \sqrt[3]{4} \\
T_5(\sqrt[3]{2}) &= 5\sqrt[3]{2} = 0 \cdot 1 + 5 \cdot \sqrt[3]{2} + 0 \cdot \sqrt[3]{4} \\
T_5(\sqrt[3]{4}) &= 5\sqrt[3]{4} = 0 \cdot 1 + 0 \cdot \sqrt[3]{2} + 1 \cdot \sqrt[3]{4} \\
[T_5] = [5] &= \begin{pmatrix} 5 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 5 \end{pmatrix}.
\end{aligned}$$

- Use $\beta = \sqrt[3]{2}$. Then

$$\begin{aligned}
T_{\sqrt[3]{2}}(1) &= \sqrt[3]{2} \cdot 1 = \sqrt[3]{2} \\
&= 0 \cdot 1 + 1 \cdot \sqrt[3]{2} + 0 \cdot \sqrt[3]{4} \\
T_{\sqrt[3]{2}}(\sqrt[3]{2}) &= \sqrt[3]{2}\sqrt[3]{2} = \sqrt[3]{4} \\
&= 0 \cdot 1 + 0 \cdot \sqrt[3]{2} + 1 \cdot \sqrt[3]{4} \\
T_{\sqrt[3]{2}}(\sqrt[3]{4}) &= \sqrt[3]{8} = 2 \\
&= 2 \cdot 1 + 0 \cdot \sqrt[3]{2} + 0 \cdot \sqrt[3]{4} \\
[T_{\sqrt[3]{2}}] &= \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}
\end{aligned}$$

- Use $\beta = 1 + \sqrt[3]{2} + \sqrt[3]{4}$. Then

$$\begin{aligned}
T_\beta(1) &= 1 + \sqrt[3]{2} + \sqrt[3]{4} \\
T_\beta(\sqrt[3]{2}) &= (1 + \sqrt[3]{2} + \sqrt[3]{4})\sqrt[3]{2} \\
&= 2 + \sqrt[3]{2} + \sqrt[3]{4} \\
T_\beta(\sqrt[3]{4}) &= (1 + \sqrt[3]{2} + \sqrt[3]{4})\sqrt[3]{4} \\
&= 2 + 2\sqrt[3]{2} + \sqrt[3]{4} \\
[\beta] &= \begin{pmatrix} 1 & 2 & 2 \\ 1 & 1 & 2 \\ 1 & 1 & 1 \end{pmatrix}
\end{aligned}$$

Lemma

a. If $\beta \in \mathbb{Q}$, then $[\beta]$ is diagonal.

b. $[\alpha]$ is the companion matrix of $\mu_\alpha(x)$, the minimal polynomial of x.

c. $\mu_\beta(x) | \chi_{T_\beta}(x)$.

Proof □