The Arithmetic of Algebraic Numbers: An Elementary Approach

Chi-Kwong Li (ckli@math.wm.edu) and David Lutzer (lutzer@math.wm.edu).
College of William and Mary, Williamsburg, VA 23187

Let $\mathbb{Q}$ and $\mathbb{R}$ be the fields of rational and real numbers respectively. Recall that a real number r is *algebraic over the rationals* if there is a polynomial p with coefficients in $\mathbb{Q}$ that has r as a root, i.e., that has $p(r) = 0$. Any college freshman can understand that idea, but things get more challenging when one asks about arithmetic with algebraic numbers. For example, being the roots of $x^2 - 3$ and $x^2 - 20$ respectively, the real numbers $r_1 = \sqrt{3}$ and $s_1 = 2\sqrt{5}$ are certainly algebraic over the rationals, but what about the numbers $r_1 + s_1,\ r_1 s_1$ and $\frac{r_1}{s_1}$? As it happens, all three are algebraic over the rationals. For example, $r_1 + s_1$ is a root of $x^4 - 46x^2 + 289$. But how was that polynomial constructed, and what rational-coefficient-polynomials have $r_1 s_1$ and $\frac{r_1}{s_1}$ as roots? Students who take a second modern algebra course will learn to use field extension theory to show that the required polynomials must exist. They will learn that whenever r and $s \neq 0$ are algebraic over $\mathbb{Q}$, then the field $\mathbb{Q}(r,s)$ is an extension of $\mathbb{Q}$ of finite degree with the consequence that $r + s,\ rs$ and $\frac{r}{s}$ are indeed algebraic over $\mathbb{Q}$ (see [2, 3, 7]). However, one would hope that students would encounter more elementary solutions for such basic arithmetic questions. Furthermore, one might want to know how to construct rational-coefficient polynomials that have $r + s,\ rs$ and $\frac{r}{s}$ as roots and thereby obtain bounds on the minimum degrees of such polynomials.

The goal of this classroom note is to show how techniques accessible to students by the end of their first linear algebra course can answer all of these questions. Our hope is that modern algebra instructors will see such constructions as a source of student projects that tie together ideas from linear algebra and modern algebra, and as a way to study the field of algebraic numbers earlier in the usual modern algebra sequence.

We do not claim that our approach is new: the 1996 articles [5] and [1] included the same ideas. However, for some reason, these earlier articles have not led to wide-spread changes in the way textbook authors present the arithmetic of algebraic numbers. Therefore we believe that it is worth raising the ideas again.

Lemma: Suppose r and s are real numbers that are algebraic over $\mathbb{Q}$ with $s \neq 0$. Then $r + s, rs$ and $\frac{r}{s}$ are also algebraic over $\mathbb{Q}$.

Proof: Our proof uses the ideas of characteristic polynomials, eigenvalues, and eigenvectors, all of which are in the typical first linear algebra course. We also need two other ideas, namely the companion matrix of a polynomial and the Kronecker product, that typically appear in more advanced linear algebra texts (for example, see [4, 6]). Even though companion matrices and Kronecker products are not yet standard fare in beginning linear algebra courses, students from such courses can easily verify their necessary properties, described below.

1. Suppose $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ is a given a monic polynomial. Let A be the $n \times n$ matrix with 1 in the $(1,2), \ldots, (n-1,n)$ positions, the last row equals $-[a_0, a_1, \cdots, a_{n-1}]$, and all other entries zero. Then A is the known as the *companion matrix* of $p(x)$ and satisfies $p(x) = \det(xI - A)$. Moreover, if A is invertible, i.e., $a_0 \neq 0$, then A^{-1} has 1 in the

$(2,1),\ldots,(n,n-1)$ positions, the first row equals $-[a_1,\ldots,a_{n-1},1]/a_0$, and all other entries zero. For example, if $p(x)=x^3+a_2x^2+a_1x+a_0$ with $a_0\neq 0$, then

$$A=\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -a_0 & -a_1 & -a_2 \end{bmatrix} \quad \text{and} \quad A^{-1}=\begin{bmatrix} -a_1/a_0 & -a_2/a_0 & -1/a_0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

2. If A is $n\times p$ and B is $m\times q$, we can define the *Kronecker product* of A and B as $A\otimes B=(a_{ij}B)_{1\leq i\leq n,1\leq j\leq p}$. Moreover, if the dimensions are compatible, then $(A\otimes B)(C\otimes D)=(AC)\otimes(BD)$. In fact, in our application, we only use the special case when $n=p$, $m=q$, C is $p\times 1$ and D is $q\times 1$.

Using those two ideas we sketch the proof of our lemma and invite students to check the details. Suppose r and s are algebraic numbers that are roots of the rational polynomials $p(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_0$ and $q(x)=x^m+b_{m-1}x^{m-1}+\cdots+b_0$, respectively. Let A and B be the companion matrices of $p(x)$ and $q(x)$. Then $Au=ru$ for some $u\in\mathbb{R}^n$ and $Bv=sv$ for some $v\in\mathbb{R}^n$, and we have

$$(A\otimes I_m+I_n\otimes B)(u\otimes v)=(r+s)(u\otimes v), \text{ and } (A\otimes B)(u\otimes v)=(rs)(u\otimes v).$$

Thus, $r+s$ and rs are algebraic and the characteristic polynomial of $A\otimes I_m+I_n\otimes B$ and of $A\otimes B$ have them as roots.

To complete the proof, we note that $\frac{r}{s}=r*\frac{1}{s}$ so that it will be enough to show that $\frac{1}{s}$ is algebraic over $\mathbb{Q}$. We may assume that $p(x)=x^n+\cdots+a_0$ with $a_0\neq 0$; otherwise, we replace $p(x)$ by $p(x)/x^k$ for a suitable positive integer k. Then A^{-1} exists. By (1), A^{-1} is a rational matrix. Now, $1/s$ is a root of the characteristic polynomial of A^{-1}, and hence is algebraic. The proof is now complete. □

Corollary: Suppose that r and $s\neq 0$ are roots of rational-coefficient-polynomials of degrees m and n respectively. Then $r+s$, rs and $\frac{r}{s}$ are roots of rational-coefficient polynomials of degree mn. □

Remark: There is an even easier proof that $\frac{1}{s}$ is an algebraic number provided $s\neq 0$ is a root of the polynomial $a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$: simply consider the polynomial obtained by reversing the coefficient order of p, i.e., consider $q(x)=a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n$, and verify that $q(s)=0$.

Modern algebra courses generalize the notion of an algebraic number over $\mathbb{Q}$ when studying field extensions. Recall that for a subfield K of a field L, an element $r\in L$ is algebraic over K if there is a polynomial $p\in K[x]$ having r as a root. The techniques in the Lemma and Corollary above may be applied, verbatim, to elements r and $s\neq 0$ in the field L that are algebraic over the subfield K. Second, observe that the arguments above also show that the set of algebraic integers is a ring, where by an *algebraic integer* we mean any complex number that is a root of some *monic* polynomial with *integer* coefficients.

In closing, the authors would like to thank the referee whose comments greatly improved an earlier version of this paper.

References

[1] S. Fallat, Algebraic integers and the tensor product of matrices, Crux Mathematicorum, 22 (1996) 341-343.

[2] J. Fraleigh, *A First Course in Abstract Algebra*, Seventh Edition, Addison Wesley Longman, Reading MA, 2001.

[3] I.N. Herstein, *Topics in Algebra*, Second edition, Xerox College Publishing, Lexington, MA and Toronto, 1975.

[4] R. Horn and C. Johnson, *Matrix Analysis*, Cambridge University Press, Cambridge, 1985.

[5] D. Kalman, R. Mena, and S. Shahriari, Variations on an irrational theme – geometry, dynamics, algebra, *Math. Mag.* 70 (1997), 93-104.

[6] P. Lancaster and M. Tismenetsky, *The Theory of Matrices*, Second edition, Computer Science and Applied Mathematics, Academic Press, Inc., Orlando, FL, 1985.

[7] J.J. Rotman, *A First Course in Abstract Algebra*, Prentice Hall, Upper Saddle River, NJ, 1996.