These problems could make for interesting research topics for a course in game theory or for undergraduate research. We await results with anticipation.

References


The Existence of Multiplicative Inverses

Ricardo Alfaro (ralfaro@umflint.edu) and Steven C. Althoen (salthoen@umflint.edu), University of Michigan-Flint, Flint, MI 48502

It is a common in undergraduate abstract algebra courses to show that if \( c \) is square-free, the ring \( \mathbb{Q}[\sqrt{c}] \) is a field. The proof usually involves the notions of minimal irreducible polynomials, quotient fields, isomorphisms, and algebraic extensions (see [1, Ch.13] or [2, Ch.8], for example).

In this note, we show that every nonzero element in this ring has a multiplicative inverse, using only basic ideas from linear algebra and number theory.

Let \( c \) be a square-free integer. The set \( \mathbb{Q}[\sqrt{c}] \) is defined as

\[
\{a_0 + a_1 \sqrt{c} + a_2 (\sqrt{c})^2 + \cdots + a_{n-1} (\sqrt{c})^{n-1} | a_i \in \mathbb{Q} \text{ for all } i\}.
\]

Let \( a \) be a nonzero element in \( \mathbb{Q}[\sqrt{c}] \). Our problem is to find another element \( x = x_0 + x_1 \sqrt{c} + x_2 (\sqrt{c})^2 + \cdots + x_{n-1} (\sqrt{c})^{n-1} \) such that \( a \cdot x = 1 \).

By multiplying by common denominators, we see that the problem can be restated as follows:

Let \( a = a_0 + a_1 \sqrt{c} + a_2 (\sqrt{c})^2 + \cdots + a_{n-1} (\sqrt{c})^{n-1} \) with \( a_i \in \mathbb{Z} \). If \( a \neq 0 \), show that there exists an element \( x = x_0 + x_1 \sqrt{c} + x_2 (\sqrt{c})^2 + \cdots + x_{n-1} (\sqrt{c})^{n-1} \) with \( x_i \in \mathbb{Q} \) such that \( a \cdot x = m \in \mathbb{Q} \).

Furthermore, since \( a \neq 0 \), we can assume the coefficients of \( a \) are relatively prime, that is \( \gcd(a_0, a_1, \ldots, a_{n-1}) = 1 \). So, assume \( a_i \in \mathbb{Z} \), and let \( \alpha \) denote \( \sqrt{c} \). Multiply the two polynomials in the variable \( \alpha \), using the fact that \( c \) is square-free and \( \alpha^n = c \in \mathbb{Z} \).

The existence of an inverse is then equivalent to the following condition: the coefficient of \( \alpha^j \) is 0 for \( j = 1, 2, \ldots, n - 1 \), and the coefficient of \( \alpha^0 \) is some \( m \in \mathbb{Q} \). We obtain a linear system of equations in the variables \( x_i \), which written in matrix form
Hence, a multiplicative inverse for $a$ in $\mathbb{Q} \left[ \sqrt[n]{c} \right]$ exists if and only if the determinant of the coefficient matrix $A$ of this equation is nonzero.

Suppose $\det(A) = 0$. Since all of the entries in $A$ are integers, this is equivalent to having $\det(A) \equiv 0 \pmod{p}$ for every prime $p$. Consider a prime $p$ that divides $c$. Then

$$
\det(A) \equiv \det \begin{pmatrix}
    a_0 & 0 & 0 & \cdots & 0 & 0 \\
    a_1 & a_0 & 0 & \cdots & 0 & 0 \\
    a_2 & a_1 & a_0 & \cdots & 0 & 0 \\
    \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
    a_{n-2} & a_{n-3} & a_{n-4} & \cdots & a_0 & 0 \\
    a_{n-1} & a_{n-2} & a_{n-3} & \cdots & a_1 & a_0
\end{pmatrix} \equiv (a_0)^n \equiv 0 \pmod{p}.
$$

Thus $p | a_0^n$, and hence $p | a_0$ since $p$ is prime. This is true for every prime divisor of $c$, and hence $c | a_0$.

Replace $a_0$ by $d_0 c$ in the matrix $A$. We can then factor $c$ from the first row and move the first row to the bottom of the matrix, and obtain

$$
\det(A) = \det \begin{pmatrix}
    d_0 c & a_{n-1} c & a_{n-2} c & \cdots & a_2 c & a_1 c \\
    a_1 & d_0 c & a_{n-1} c & \cdots & a_3 c & a_2 c \\
    a_2 & a_1 & d_0 c & \cdots & a_4 c & a_3 c \\
    \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
    a_{n-2} & a_{n-3} & a_{n-4} & \cdots & d_0 c & a_{n-1} c \\
    a_{n-1} & a_{n-2} & a_{n-3} & \cdots & a_1 & d_0 c
\end{pmatrix}
$$

$$
= (c)(-1)^{n-1} \det \begin{pmatrix}
    a_1 & d_0 c & a_{n-1} c & \cdots & a_3 c & a_2 c \\
    a_2 & a_1 & d_0 c & \cdots & a_4 c & a_3 c \\
    \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
    a_{n-1} & a_{n-2} & a_{n-3} & \cdots & a_1 & d_0 c \\
    d_0 & a_{n-1} & a_{n-2} & \cdots & a_2 & a_1
\end{pmatrix} = 0.
$$

Since $\gcd(a_0, a_1, \ldots, a_{n-1}) = 1$, it follows that $\gcd(a_1, \ldots, a_{n-1}, d_0) = 1$, and we can repeat the process with this last matrix. Therefore $c | a_1$. Continuing in the same way, we deduce that $c | a_i$, for all $i = 1, 2, \ldots, n - 1$; which is a contradiction, since $\gcd(a_0, a_1, \ldots, a_{n-1}) = 1$.

Thus, the determinant of the coefficient matrix is nonzero, and $a$ has a multiplicative inverse in $\mathbb{Q} \left[ \sqrt[n]{c} \right]$.

References