# When Does a Quadratic Extension Field Contain $\sqrt{-1}$?

Walden Freedman (wf6@humboldt.edu), Humboldt State University, Arcata, CA 95521

The complex number $i$ which satisfies $i^2 = -1$ is familiar to most undergraduate mathematics students. Students taking abstract algebra encounter other fields which contain similar elements such as the extension field $\mathbb{Z}_3[x]/\langle x^2 + 1\rangle$. Although this field contains only 9 elements, it also contains an element whose square is $-1$, that is, whose square is the additive inverse of the unity element of the field. If $k$ is a field we will write $\sqrt{-1} \in k$ to mean that such an element of $k$ exists.

Our purpose is to answer the following question: Under what conditions does a quadratic extension field contain $\sqrt{-1}$? This question and its solution are not commonly included in undergraduate algebra courses or texts, but are readily accessible. While this result is of interest in its own right, it also suggests further avenues of research suitable for undergraduates. We give several questions at the end of the paper as a starting point. These ideas occured to the author who is an analyst, not an algebraist, after teaching a two-semester course in abstract algebra.

Recall that if $k$ is a field, and $f(x) \in k[x]$ is irreducible, then there is a field extension $K$ of $k$ in which $f(x)$ has a root $z$. In particular, if $I = \langle f(x)\rangle$ is the ideal of $k[x]$ generated by $f(x)$, then we may take $K = k[x]/I$, with $z = x + I$. If $f(x)$ is a quadratic, then $K$ is a quadratic extension field, and we may write $K = k(z)$, the field generated by $k$ and the element $z$. In particular, $K = \{\alpha + \beta z : \alpha, \beta \in k\}$.

The condition under which a second degree polynomial with real coefficients has no real root should be familiar to undergraduate mathematics students. With reference to the quadratic formula, if $f(x) = ax^2 + bx + c$ with $a, b, c \in \mathbb{R}$, (and $a \neq 0$), then $f$ has no real root if and only if $b^2 - 4ac < 0$.

Students of abstract algebra may be pleased to learn that there is also a version of this condition which holds over more general fields, specifically, those not of characteristic 2. We introduce the following notation: For a commutative ring $R$, let $\mathrm{Sq}(R) = \{r^2 : r \in R\}$, the set of all squares of elements of $R$. Clearly, for $c \in R$, we have $\sqrt{c} \in R$ if and only if $c \in \mathrm{Sq}(R)$. In particular, $\sqrt{-1} \in k$ iff $-1 \in \mathrm{Sq}(k)$.

**Lemma.** *Let $k$ be field with* $\mathrm{char}(k) \neq 2$. *The quadratic polynomial $ax^2 + bx + c \in k[x]$ has no roots in $k$, and hence is irreducible over $k$, if and only if $b^2 - 4ac \notin \mathrm{Sq}(k)$.*

The proof of the lemma comes from the usual process of completing the square. Since $\mathbb{R}$ always contains the square roots of nonnegative real numbers, this leads to the familar result for quadratics with real coefficients mentioned above. It also suggests that the set $\mathrm{Sq}(k)$ deserves further study.

For example, the quadratic $f(x) = 2x^2 + 2x + 1$ is irreducible over $k = \mathbb{Z}_7$, for writing $k = \{0, 1, 2, 3, 4, 5, 6\}$, we find $\mathrm{Sq}(k) = \{0, 1, 4, 2\}$. Hence with $a = 2, b = 2$, and $c = 1$, we have $b^2 - 4ac = 3 \notin \mathrm{Sq}(k)$. Now, let $z$ be a root of $f(x)$ in an extension field $K$. Since $f(x)$ is reducible over $K$, it follows from the lemma that $b^2 - 4ac = 3 \in \mathrm{Sq}(K)$. In particular, the element $r = 2 + 4z$ satisfies $r^2 = 3$. This can be seen by squaring and substituting for $z^2$. But $4ac - b^2 = -3 = 4 = 2^2 \in \mathrm{Sq}(k)$, so that the element $\omega = 2^{-1}(2 + 4z) = 1 + 2z$ satisfies $\omega^2 = -1 \in \mathrm{Sq}(K)$, while $-1 = 6 \notin \mathrm{Sq}(k)$. This fact follows more generally from the theorem below, which answers the question posed in the introduction. It should be noted that the theorem follows as a corollary from the main result of [**4**], as well as from Theorem 3.4 of [**2**]. However, both of these, especially [**2**], use algebraic techniques that are more sophisticated than those employed here.

 © THE MATHEMATICAL ASSOCIATION OF AMERICA

**Theorem.** *Let $k$ be a field which does not contain $\sqrt{-1}$. Let $f(x) = ax^2 + bx + c$ be irreducible in $k[x]$, with $a \neq 0$. Let $z$ be a root of $f(x)$ in some extension of $k$, and set $K = k(z)$. Then $K$ contains $\sqrt{-1}$ if and only if $4ac - b^2 \in \mathrm{Sq}(k)$.*

*Proof.* Recall that we may write $K = \{\alpha + \beta z : \alpha, \beta \in k\}$. Suppose $K$ contains an element $y$ such that $y^2 = -1$. We can then write $y = \alpha + \beta z$. Using the fact that $az^2 + bz + c = 0$, we find by squaring and substituting for $z^2$ that

$$\begin{aligned} -1 = y^2 = (\alpha + \beta z)^2 &= \alpha^2 + \beta^2 z^2 + 2\alpha\beta z \\ &= \alpha^2 + \beta^2(-a^{-1}(bz + c)) + 2\alpha\beta z \\ &= (\alpha^2 - a^{-1}c\beta^2) + z(2\alpha\beta - a^{-1}b\beta^2). \end{aligned}$$

Hence, we have

$$\begin{aligned} -1 &= \alpha^2 - a^{-1}c\beta^2, \quad \text{and} \\ 0 &= 2\alpha\beta - a^{-1}b\beta^2. \end{aligned}$$

Now, $\beta \neq 0$, else $\sqrt{-1} \in k$, so the second equation implies that $\alpha = (2a)^{-1}b\beta$. Thus,

$$\begin{aligned} -1 &= (2a)^{-2}b^2\beta^2 - a^{-1}c\beta^2 \\ &= \beta^2(2a)^{-2}(b^2 - a^{-1}c(2a)^2) \\ &= \beta^2(2a)^{-2}(b^2 - 4ac). \end{aligned}$$

Hence, $4ac - b^2 = (2a\beta^{-1})^2 \in \mathrm{Sq}(k)$, as desired.

Conversely, suppose that $4ac - b^2 \in \mathrm{Sq}(k)$. Since $k \subseteq K$, $4ac - b^2 \in \mathrm{Sq}(K)$. Now, $f(t) = at^2 + bt + c$ is reducible in $K[t]$, so it follows from the lemma that $b^2 - 4ac \in \mathrm{Sq}(K)$. But this means that their quotient, $-1$, is in $\mathrm{Sq}(K)$, as desired. (Alternatively, one can show that if $r \in k$ satisfies $r^2 = 4ac - b^2$, then setting $\omega = r^{-1}(b + 2az) \in K$, we have $\omega^2 = -1 \in K$.) ∎

Undergraduates are more familiar with extension fields where $k = \mathbb{R}$. Combining the results of the lemma and the theorem in this setting gives the following corollary.

**Corollary.** *If $f(x) = ax^2 + bx + c \in \mathbb{R}[x]$ is irreducible, then $\mathbb{R}[x]/\langle f(x)\rangle$ contains $\sqrt{-1}$.*

**Note.** The assumption that $\sqrt{-1} \notin k$ is necessary in the theorem. Take $k = \mathbb{Q}(i) = \{\alpha + \beta i : \alpha, \beta \in \mathbb{Q}\}$, where $i \in \mathbb{C}$ as usual. (Equivalently, $k$ is the extension field $\mathbb{Q}[t]/\langle t^2 + 1\rangle$.) Now, $x^2 - 2$ is irreducible over $k$, and $K = k(\sqrt{2})$ contains $\sqrt{-1}$, since $k$ contains it, but in this case, $4ac - b^2 = -8$, and if $(\alpha + \beta i)^2 = -8$, we find $\alpha^2 - \beta^2 = -8$, and $\alpha\beta = 0$, which is impossible since $\alpha, \beta \in \mathbb{Q}$.

We end with some questions. They and the references are meant as a starting point for beginning researchers. The answers are unknown to the author, but may possibly be available in the literature.

(a) Characterize fields $k$ such that $\mathrm{Sq}(k) = k$. If $\mathrm{char}(k) \neq 2$, must $\mathrm{char}(k) = 0$?

(b) Let $k$ be an infinite field such that $-1 \notin \mathrm{Sq}(k)$. Find conditions on an irreducible polynomial $f \in k[x]$ implying that $k[x]/\langle f(x)\rangle$ contains $\sqrt{-1}$.

(c) Let $p$ be an odd prime, and let $\phi_p(x)$ denote the $p$th cyclotomic polynomial. Does $\mathbb{Q}[x]/\langle\phi_p(x)\rangle$ contain $\sqrt{-1}$?

*Acknowledgment.* The author is grateful to the referees for their helpful suggestions.

## References

1. L. Childs, *A Concrete Introduction to Higher Algebra*, Springer-Verlag, New York, 2000.
2. T. Y. Lam, *The Algebraic Theory of Quadratic Forms*, W. A. Benjamin, Inc., 1973.
3. S. Lang, *Algebra*, Springer-Verlag, New York, 2002.
4. C. Parry and D. Perin, Equivalence of extension fields, *Math. Mag.* **50** (1) (1977) 36–38.

 © THE MATHEMATICAL ASSOCIATION OF AMERICA