Proving the irreducibility of $x^4 + 1$

One of the common threads of the part of the course that is showing up on midterm 3 is the recurring question of how to determine that a polynomial is irreducible.

Keep in mind that in general, determining whether an element of a ring is irreducible is a very hard problem! Determining which integers are prime is actually a special case of this problem. Deciding whether a given integer is prime becomes very computationally intensive (this difficulty is what makes RSA a successful way of protecting our data), and finding new prime numbers, especially in order, is also incredibly difficult.

So, it stands to reason that determining if a polynomial is irreducible is a hard problem, and there isn’t any one technique that we can use all the time, but rather a variety of techniques.

**Problem:** Show that $x^4 + 1$ is irreducible over $\mathbb{Q}$.

**An idea that is helpful but not enough:** Note carefully that it is not sufficient to show that the roots of $x^4 + 1$ in $\mathbb{C}$, which are $\zeta_8$, $\zeta_8^3$, $\zeta_8^5$, $\zeta_8^7$, are not in $\mathbb{Q}$. This argument has ruled out the possibility of $x^4 + 1$ having any linear factors in $\mathbb{Q}$, but has not ruled out the possibility that it could be written as a product of two degree-2 polynomials with coefficients in $\mathbb{Q}$. It would then be possible to finish the argument by showing that any product of two of the linear factors of $x^4 + 1$ in $\mathbb{C}[x]$, which are $x - \zeta_8$, $x - \zeta_8^3$, $x - \zeta_8^5$, $x - \zeta_8^7$, does not have coefficients in $\mathbb{Q}$. However, this last step is rather a lot of computational work and other methods are probably easier to use and more broadly applicable to other situations. Some suggestions are listed below.

**Possible Approach: Eisenstein’s Criterion:** Although we can’t use Eisenstein’s criterion directly, the method we used to prove that $x^{p-1} + \cdots + x + 1$ is irreducible for any prime $p$ can also be applied here.

Substituting in $y + 1$ for $x$ yields

$$(y + 1)^4 + 1 = y^4 + 4y^3 + 6y^2 + 4y + 2$$

Every coefficient other than the leading one is divisible by 2 and the constant term isn’t divisible by $2^2$, so Eisenstein’s criterion tells us that $y^4 + 4y^3 + 6y^2 + 4y + 2$ is irreducible.

It’s important to understand why proving that $y^4 + 4y^3 + 6y^2 + 4y + 2$ is irreducible implies that $x^4 + 1$ is irreducible. What we’ve done is apply the ring isomorphism $\mathbb{Q}[x] \to \mathbb{Q}[y]$ that sends the coefficients to themselves and sends $x$ to $y + 1$. If $x^4 + 1$ could be factored nontrivially, then the isomorphism would send those factors to factors of $y^4 + 4y^3 + 6y^2 + 4y + 2$ and they would be nontrivial factors since our ring isomorphism preserves the degree of polynomials.

**Possible Approach: Complex conjugates of roots and some extra arguing:** This problem came to us initially as part of finding the irreducible polynomial of $\zeta_8 := e^{2\pi i/8}$ over $\mathbb{Q}$. We can see that $\bar{\zeta}_8 := e^{2\pi i/8}$ is certainly a root of $x^8 - 1 = (x^4 + 1)(x^4 - 1)$. The roots of the factor $x^4 - 1$ in $\mathbb{C}$ are $\pm 1$ and $\pm i$, and so $\zeta_8$ is a root of $x^4 + 1$. Call $f(x)$ the irreducible polynomial of $\text{zeta}_8$ over $\mathbb{Q}$. To show that $x^4 + 1$ is irreducible over $\mathbb{Q}$ it suffices to show that that $f(x) = x^4 + 1$.

**Helpful result: see 15.4 or, better, 16.4 in the book:** Let $K/F$ be a field extension. Recall that if a polynomial $p(x)$ has coefficients in $F$ and a root $\alpha$ in $K$, then any $K$-automorphism $\varphi$ of $F$ will send $\alpha$ to a (potentially different) root of $p(x)$:

$$p(\alpha) = 0, \text{ so } \varphi(p(\alpha)) = \varphi(0) = 0, \text{ and since } \varphi \text{ acts as the identity on elements of } F, \varphi(p(\alpha)) = p(\varphi(\alpha))$$

Since complex conjugation is a $\mathbb{Q}$-automorphism (and also an $\mathbb{R}$-automorphism) of $\mathbb{C}$, the complex conjugate $\bar{\zeta}_8 = \zeta_8^4$ must also be a root of $f(x)$. This tells us that $f(x)$ must have degree at least 2.

Now, we can use our helpful result again to find other roots (shown below), or we can argue more directly: we know that $(x - \zeta_8)(x - \bar{\zeta}_8)$ must be a factor of $f(x)$, but $(x - \zeta_8)(x - \bar{\zeta}_8) = x^2 - \sqrt{2}x + 1$ does not have coefficients in $\mathbb{Q}$. So, $f(x)$ must have degree strictly greater than 2. Since $f(x)$ divides $x^4 + 1$, the degree of $f(x)$ is at most 4, and if it’s equal to 4, $f(x) = x^4 + 1$ and we are done. The only case we have to eliminate
is the case where the degree of \( f(x) \) is 3. But if \( f(x) \) were degree 3, then its other factor would have to be \( \zeta_8^2 \) or its complex conjugate \( \zeta_8^5 \), but those are both complex, and so \( f(x) \) would have to have both of them as roots, ruling our the possibility of \( f(x) \) having degree 3.

**Possible Approach: More automorphisms of fields** (Thanks to Jack for the suggestion on the revision)

We could take a slightly different route to finishing the last argument by showing that there is a \( \mathbb{Q} \)-automorphism of \( \mathbb{Q}(\zeta_8) \) that sends \( \zeta_8 \) to \( \zeta_8^5 \) and using the helpful result and the fact that the complex conjugates of both \( \zeta_8 \) and \( \zeta_8^5 \) must both also be factors of the irreducible polynomial of \( \zeta_8 \).

The work we must do here is to check that such a field automorphism exists. It’s a little tricky here since we don’t know what a basis of \( \mathbb{Q}(\zeta_8) \) as a \( \mathbb{Q} \)-vector space is since we don’t know the degree of \( [\mathbb{Q}(\zeta_8) : \mathbb{Q}] \).

However, we can use the fact that \( \mathbb{Q}(\zeta_8) = \mathbb{Q}(i, \sqrt{2}) \). The basis for \( \mathbb{Q}(i, \sqrt{2}) \) over \( \mathbb{Q}(i) \) is \( \{1, \sqrt{2}\} \). We’d have to do a little checking to show it exists (thing along the lines of our argument in class showing complex conjugation is the only \( \mathbb{R} \)-automorphism of \( \mathbb{C} \), but there is a ring automorphism of \( \mathbb{Q}(i, \sqrt{2}) \) that sends \( \sqrt{2} \) to \( -\sqrt{2} \) and 1 to itself. This map is a \( \mathbb{Q}(i) \)-automorphism and hence a \( \mathbb{Q} \)-automorphism and will send \( \zeta_8 \) to \( -\zeta_8 \).

**Possible Approach: Degree of a field extension by finding sub-extensions**  Again, to show that \( x^4 + 1 \) is irreducible over \( \mathbb{Q} \), it suffices to show that the irreducible polynomial of \( \zeta_8 \) over \( \mathbb{Q} \) has degree 4 since we already know that it divides \( x^4 + 1 \). We could do this by showing that \( [\mathbb{Q}(\zeta_8) : \mathbb{Q}] = 4 \) by producing a helpful intermediate field extension.

Note that \( \mathbb{Q}(i) \) is a subfield of \( \mathbb{Q}(\zeta_8) \) since \( \zeta_8^2 = i \). We have that \( [\mathbb{Q}(\zeta_8) : \mathbb{Q}] = [\mathbb{Q}(\zeta_8) : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}] \).

We know that \( [\mathbb{Q}(i) : \mathbb{Q}] = 2 \) since the irreducible polynomial of \( i \) over \( \mathbb{Q} \) is \( x^2 + 1 \), which we can show using the fact that \( i \) is a root and so its complex conjugate must also be a root (see the “helpful result” above).

We could show this other ways as well.

Since \( [\mathbb{Q}(\zeta_8) : \mathbb{Q}] \leq 4 \), using that \( [\mathbb{Q}(\zeta_8) : \mathbb{Q}] = [\mathbb{Q}(\zeta_8) : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}] = [\mathbb{Q}(\zeta_8) : \mathbb{Q}(i)] \cdot 2 \), we know that \( [\mathbb{Q}(\zeta_8) : \mathbb{Q}(i)] \) is either 1 or 2. To show \( [\mathbb{Q}(\zeta_8) : \mathbb{Q}] = 4 \), it suffices to show that \( [\mathbb{Q}(\zeta_8) : \mathbb{Q}(i)] = 2 \), so to complete our argument we just need to show that \( \mathbb{Q}(i) \) is properly contained in \( \mathbb{Q}(\zeta_8) \). For instance, \( 2\zeta_8 = \sqrt{2}(1 + i) \). Since \( \{1, i\} \) is a basis for \( \mathbb{Q}(i) \) over \( \mathbb{Q} \), any element in it can be written (uniquely) as \( a + bi \) for some \( a, b \in \mathbb{Q} \).

But, for these numbers to be equal, their real parts would have to be equal, implying \( \sqrt{2} = a \), but we assumed \( a \) is irrational so this gives a contradiction.

Other methods of proof may also work!