1. *Proof.*

(a) The factorization of $x^m - 1$ in $\mathbb{Z}[x]$ is given by

$$x^m - 1 = \prod_{d|m} \Phi_d(x) = \Phi_m(x) \prod_{\substack{d|m \\ d\neq m}} \Phi_d(x).$$

(as seen in the notes or in Dummit and Foote) Evaluating the above at $x = a$, we have

$$a^m - 1 = \Phi_m(a) \prod_{\substack{d|m \\ d\neq m}} \Phi_d(a);$$

by reducing modulo p, since $\Phi_m(a) \equiv 0 \mod p$, we have

$$a^m - 1 = \Phi_m(a) \prod_{\substack{d|m \\ d\neq m}} \Phi_d(a) \equiv 0 \mod p.$$

If a was not relatively prime to p, then $p \mid a$ so that $a^m - 1 \equiv -1$, which by the above cannot happen. Hence a is relatively prime to p; i.e., $a \in \mathbb{F}_p^\times$.

We show the order of a in $\mathbb{F}_p^\times$ is m: Certainly the order of a divides m since $a^m - 1 \equiv 0 \mod p$; suppose by contradiction that a had order j dividing m with $j < m$. Then $a^j - 1 = \prod_{d|j} \Phi_d(a) = 0$, so there is some $d' \mid j$ with $\Phi_{d'}(a) = 0$. But $x^j - 1 = \prod_{d|j} \Phi_d(x)$ is a factor of $x^m - 1 = \prod_{d|m} \Phi_d(x)$ since $j \mid m$. Since $d' \neq m$ it follows that $x^m - 1$ has a multiple root at a over $\mathbb{F}_p$ ($\Phi_{d'}(a) = \Phi_m(a) = 0$). This is in contradiction to the separability of $x^m - 1$ over $\mathbb{F}_p$, as $x^m - 1$ is coprime with $mx^{m-1} \neq 0$ since $p \nmid m$. Thus a has order exactly m in $\mathbb{F}_p$.

(b) We show that if p does not divide m, then $p \equiv 1 \mod m$. In this case a has order m by part (a). Since $\mathbb{F}_p^\times$ has order $\phi(p) = p - 1$, the order of a divides $p - 1$. So $cm + 1 = p$ for some integer c, from which it follows that $p \equiv 1 \mod m$.

Hence p divides m or $p \equiv 1 \mod m$.

(c) By prime factorization, there are finitely many primes dividing m. Since $f(x) = x^m - 1$ is a nonconstant monic polynomial, there are infinitely many (odd) primes which are divisors of at least one of $f(1)$, $f(2)$, $f(3)$, $f(4), \ldots$. Only finitely many of these primes could divide m, so for the remaining infinitely many primes they must be congruent to 1 modulo p by part (b).

Hence there are infinitely many primes p such that $p \equiv 1 \mod m$. □

2.

(a) We use the bonus characterization of Galois extensions from the notes: The finite separable extension K/F is Galois if and only if every embedding of K into L fixing F is an automorphism of K fixing F (note every automorphism of K fixing F may be viewed as an embedding). It follows then that $N_{K/F}(\alpha) = \prod_{\sigma\in \mathrm{Gal}(K/F)} \sigma(\alpha)$ since $\mathrm{Gal}(K/F)$ is the group of all automorphisms of K fixing F.

(b) Let $G = \mathrm{Gal}(L/F)$ and $H = \mathrm{Gal}(L/K)$. By the Galois correspondence (from notes/Dummit and Foote), the embeddings of K into L fixing F are in bijective correspondence with the cosets σH of G/H. So $N_{K/F}(\alpha) = \prod_{\sigma H \in G/H} \sigma(\alpha)$.

We recall that G acts transitively by multiplication on G/H: Given $\sigma H, \tau H$, since G is a group find σ' such that $\sigma'\sigma = \tau$ so that $\sigma'(\sigma H) = (\sigma'\sigma)H = \tau H$. Thus $g(G/H)$ is in bijection with G/H (the multiplication permutes the cosets).

Then consider the polynomial $f(x) = \prod_{\sigma H \in G/H}(x - \sigma(\alpha)) \in K[x]$. For any element $\tau \in G$ we extend τ to a map on $K[x]$ by letting τ be a homomorphism such that $x \mapsto x$. Then $\tau(f(x)) = \prod_{\sigma H \in G/H}(x - (\tau\sigma)(\alpha)) = \prod_{\sigma H \in G/H}(x - \sigma(\alpha))$ since multiplication by τ simply permutes the cosets σH (and we do not need to worry about which coset representatives we end up with after the multiplication since they differ by a factor in H, but H fixes K). Since τ was arbitrary, it follows that G fixes $f(x)$, meaning all of the coefficients of $f(x)$ actually were in F. So $f(x) \in F[x]$, and observe that $\prod_{\sigma H \in G/H} \sigma(\alpha)$ is, up to a sign, the constant term of $f(x)$, which is in F as desired.

(c) Each of the embeddings are homomorphisms, so

$$N_{K/F}(\alpha\beta) = \prod_{\sigma} \sigma(\alpha\beta) = \prod_{\sigma} \sigma(\alpha)\sigma(\beta) = \prod_{\sigma} \sigma(\alpha) \prod_{\sigma} \sigma(\beta) = N_{K/F}(\alpha)N_{K/F}(\beta).$$

(d) Since $F(\alpha)$ is a subfield of K containing F and $m_\alpha(x)$ is degree d (so $[F(\alpha)\colon F] = d$), it follows by the tower law that $n = [K\colon F] = [K\colon F(\alpha)][F(\alpha)\colon F] = [K\colon F(\alpha)]d$. Hence $d \mid n$.

Observe that the minimal polynomial $m_\alpha(x)$ divides $\prod_{\sigma H \in G/H}(x - \sigma(\alpha))$ since α is a root of the latter. It follows that there is a product $\prod_{i=1}^{d}(x - \sigma_i(\alpha))$ of d distinct factors (since K is a separable extension $m_\alpha(x)$ has distinct roots) with $\prod_{i=1}^{d}(x - \sigma_i(\alpha)) = m_\alpha(x)$, where σ_i are coset representatives for d of the cosets in G/H and $\sigma_1 = \mathrm{id}_K$.

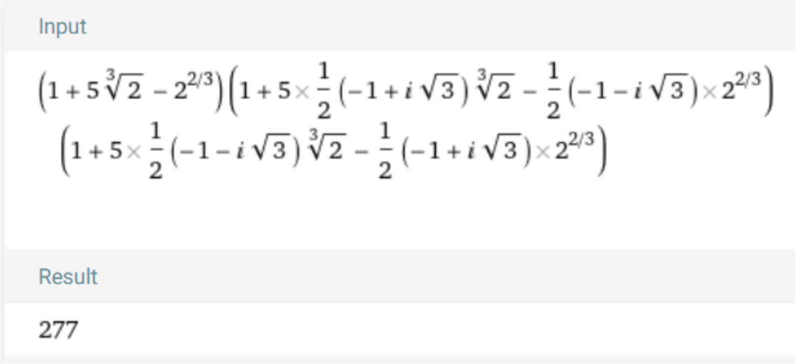
Observe further that since $m_\alpha(x)$ is over F, that any embedding of K into L fixing F will only permute the factors of the product. Consider a representative σ of some coset σH not equal to $\sigma_i H$ for $1 \leq i \leq d$. Then the product $\prod_{i=1}^{d}(x - \sigma\sigma_i(\alpha))$ is equal to $m_\alpha(x)$ but appears as a factor of $\prod_{\sigma H \in G/H}(x - \sigma(\alpha))$ distinct from $\prod_{i=1}^{d}(x - \sigma_i(\alpha)) = m_\alpha(x)$ (so $m_\alpha(x)$ is a repeated factor in the whole product). We should be able to iterate this process (by finding successive embeddings σ such that $\prod_{i=1}^{d}(x - \sigma\sigma_i(\alpha))$ are distinct from the ones already found) to find $m_\alpha(x)$ as a repeated factor of $\prod_{\sigma H \in G/H}(x - \sigma(\alpha))$ exactly n/d times since $|G/H| = [K\colon F] = n$ by the Galois correspondence.

Then see that with $x = 0$, we have $a_0^{n/d} = m_\alpha(0)^{n/d} = \prod_{\sigma H \in G/H}(-\sigma(\alpha)) = (-1)^n N_{K/F}(\alpha)$. Therefore the d distinct roots of $m_\alpha(x)$ are the d distinct Galois conjugates of α which appear as repeated factors of $N_{K/F}(\alpha)$, and by multiplying the above equality by $(-1)^n$ on both sides obtain $N_{K/F}(\alpha) = (-1)^n a_0^{n/d}$.

3. Exam questions can be fun.

(a) Since norms are multiplicative, if α was a square of an element β in K then its norm is necessarily a square of a rational number: $N_{K/\mathbb{Q}}(\alpha) = N_{K/\mathbb{Q}}(\beta^2) = N_{K/\mathbb{Q}}(\beta)^2$, and $N_{K/\mathbb{Q}}(\beta) \in \mathbb{Q}$.

However, using Wolfram Alpha the norm of α is computed to be 277: The Galois group G of $\mathbb{Q}(\zeta_3, \sqrt[3]{2})/\mathbb{Q}$ (the splitting field of $x^3 - 2$) is given by $\langle \sigma, \tau \rangle \cong S_3$ (notations as in Dummit and Foote), where σ is the map which fixes ζ_3 and sends $\sqrt[3]{2}$ to $\zeta_3 \sqrt[3]{2}$ (order 3), and τ fixes $\sqrt[3]{2}$ and sends ζ_3 to ζ_3^2 (order 2). The subgroup $\langle \tau \rangle$ is the fixed field for $\mathbb{Q}(\sqrt[3]{2})$, from which it follows we use the three coset representatives in G/H coming from $\langle \sigma \rangle$ to compute the norm.



Input

$$\left(1+5\sqrt[3]{2}-2^{2/3}\right)\left(1+5\times\frac{1}{2}(-1+i\sqrt{3})\sqrt[3]{2}-\frac{1}{2}(-1-i\sqrt{3})\times 2^{2/3}\right)\left(1+5\times\frac{1}{2}(-1-i\sqrt{3})\sqrt[3]{2}-\frac{1}{2}(-1+i\sqrt{3})\times 2^{2/3}\right)$$

Result

277

Since 277 (it is prime as checked by computer) is not a square of a rational number, we cannot have that α is a square of an element in K. Hence $x^2 - \alpha$ is irreducible over K (it has no roots in K).

(b) If n is a sum of two integer squares $x^2 + y^2$ then n may be given by the norm of $x + iy \in \mathbb{Q}(i)$, which is $(x + iy)(x - iy) = x^2 + y^2$. [$\mathbb{Q}(i)/\mathbb{Q}$ is a quadratic Galois extension and hence only has complex conjugation as a nontrivial element in its Galois group.]

So if $n = N_{\mathbb{Q}(i)/\mathbb{Q}}(x + iy)$ and $m = N_{\mathbb{Q}(i)/\mathbb{Q}}(a + ib)$ for $x, y, a, b \in \mathbb{Z} \subset \mathbb{Q}$, then with the norm being multiplicative we have $nm = N_{\mathbb{Q}(i)/\mathbb{Q}}((x + iy)(a + ib))$. But $(x + iy)(a + ib) = (ax - by) + i(bx + ay)$ with $ax - by, bx + ay \in \mathbb{Z}$. It follows that nm is also a sum of two integer squares. [I suppose we could have also directly taken the product $nm = (x + iy)(x - iy)(a + ib)(a - ib)$ and shown it is a sum of squares of integers.]

(c) It suffices to produce one such solution; in particular, to produce one element of $\mathbb{Q}(\sqrt{3})$ whose norm is 1. Observe that the norm of $a + \sqrt{3}b \in \mathbb{Q}(\sqrt{3})$ for $a, b \in \mathbb{Z} \subset \mathbb{Q}$ is $a^2 - 3b^2$. So a, b satisfy $a^2 - 3b^2 = 1$ if and only if $a + \sqrt{3}b$ has norm 1. [$\mathbb{Q}(\sqrt{3})/\mathbb{Q}$ is a quadratic Galois extension with $\sqrt{3} \mapsto -\sqrt{3}$ as the nonidentity element of its Galois group.]

We have that the norm of $2 + \sqrt{3}$ is $(2 + \sqrt{3})(2 - \sqrt{3}) = 4 - 3 = 1$. Then consider $(2 + \sqrt{3})^2 = 7 + 4\sqrt{3} \in \mathbb{Q}(\sqrt{3})$, which also has norm 1 since the norm is multiplicative. Iterate this process.

By taking positive integer powers of $2 + \sqrt{3}$ one ought to find an infinite family of elements of the form $a + \sqrt{3}b$ with $a, b \in \mathbb{Z}$ whose norm is 1 (as the norm is multiplicative). When taking powers of $2 + \sqrt{3}$ we only obtain integer coefficients for 1 and $\sqrt{3}$ by the binomial formula or induction. We check that each power is distinct. If $(2 + \sqrt{3})^k = (2 + \sqrt{3})^j$ with $k > j \geq 1$ then $(2 + \sqrt{3})^{k-j} = 1$ which is impossible. [If we want to think about ordering of real numbers, any positive integer power of $2 + \sqrt{3}$ is strictly greater than 1.] Hence $\left\{(2 + \sqrt{3})^k \mid k \in \mathbb{Z}_+\right\}$ is an infinite set of elements of $\mathbb{Z}(\sqrt{3}) \subset \mathbb{Q}(\sqrt{3})$ which have norm 1; equivalently, each element $a + \sqrt{3}b$ in the above set produces a unique pair a, b of integers which satisfy $a^2 - 3b^2 = 1$.

Hence $x^2 - 3y^2 = 1$ has infinitely many integer-valued solutions.

4. Feedback: I thought this was pretty challenging, and I did not figure out everything. I don't know why the primes in the first problem had to be odd and my first guess is to think that something might go wrong in characteristic 2. The second question was also definitely harder and I am not sure how to fix the proof for the last part in particular as it is very scuffed. But the third problem didn't seem too bad unless somehow I missed something very big in each part.

   I didn't find any of the topics boring but some were certainly more interesting than others: I found the segments on cyclotomic field extensions and Kummer theory pretty neat as well as of course the actual Galois correspondence and the many ways one could use it, but things like dealing with finite fields seemed less interesting to me, perhaps because we did not spend as much time working with them. I don't seem to remember the difficulty varying too much between the topics.

   I am excited to learn category theory from the perspective of an algebraist, since it would be different from whatever I've seen in my topology classes.