# Galois Theory

Course Notes

22 February 2016 – 24 April 2016

# 1 About This Course

## 1.1 Suggested Reading

**S. Lang, *Algebra* (3rd ed., 2002)** Contains many exercises. Parts V, VI, and VII are especially relevant.

**R. Elkik, *Cours d'algebre* (2002)** In French. Closest in content to this course.

**J. S. Milne, *Fields and Galois Theory* (2015)** Course notes. Available for free on the Web at http://www.jmilne.org/math/CourseNotes/ft.html. The last three chapters contain "interesting and important material" not covered in the course.

**I. Stewart, *Galois Theory* (2015)** Less technically ambitious than this course, but includes history, and other applications such as ruler-and-compass constructions.

# 2 Week 1 Notes: 22 Feb – 28 Feb

## 2.1 Field extensions. Examples.

This course assumes a basic knowledge of abstract algebra (groups, rings, fields, modules), and linear algebra. All rings we consider will be associative, commutative, and with unity.

### 2.1.1 Two definitions of field extension.

Let $K$ and $L$ be fields.

**Definition 1.** We say that $L$ is an **extension of** $K$ if $K \subset L$. That is, $K$ is a subfield of $L$. Equivalently, $L$ is an extension of $K$ if $L$ is a $K$**-algebra**—in other words, if we have $(k_1\mathbf{a_1})(k_2\mathbf{a_2}) = k_1k_2\mathbf{a_1}\mathbf{a_2}$ for $k_i \in K$ and $\mathbf{a_i} \in A$.

Why are these definitions equivalent? In fact, given a $K$-algebra structure on a ring $A$, this is the same as having a homomorphism of rings $f : K \to A$. So if we have a $K$-algebra, define a homomorphism $f$ by setting $f(k) = k\mathbf{1}$ for $k \in K$. Conversely, given an arbitrary homomorphism $f : K \to A$, set $k\mathbf{a} = f(k)\mathbf{a}$ for $\mathbf{a} \in A$.

Suppose now that $A = L$ a field. Then any homomorphism $f : K \to L$ is injective. There are several ways to see this; for example, we can show that $f(k)$ is always invertible. Indeed, $\mathbf{1} = f(1) = f(kk^{-1}) = f(k)f(k^{-1})$ for any $k \neq 0$, so $f(k) \neq \mathbf{0}$ whenever $k$ is nonzero. Alternatively, we know that the kernel of $f$ is always an ideal. But $L$ is a field, so the only ideals of $L$ are $(0)$ and $(1) = K$.

### 2.1.2 Three examples.

**Example 1.** $\mathbb{C}$ is an extension of $\mathbb{R}$, and $\mathbb{R}$ is an extension of $\mathbb{Q}$.

**Example 2.** If $L$ is a field, then either (a) $1 + 1 + \ldots + 1 \neq 0$ for any sum of 1's. Then $L$ has characteristic 0 and so we have $\mathbb{Z} \subset L$, which means $\mathbb{Q} \subset L$. Then $L$ is an extension of $\mathbb{Q}$. Alternatively, suppose (b) $1 + 1 + \cdots + 1 = 0$ for some finite $m$ number of terms. The minimal such number for which this is true turns out to necessarily be a prime, $p$. We then say that $L$ has characteristic $p$, and so we have $\mathbb{Z}/p\mathbb{Z} \subset L$; $\mathbb{Z}/p\mathbb{Z}$ is a field, and we denote it (with field structure) by $\mathbb{F}_p$. In this case $L$ is an extension of $\mathbb{F}_p$. We call $\mathbb{Q}$ and $\mathbb{F}_p$ the **prime fields**: any field is an extension of a prime field, and prime fields don't contain any proper subfields.

**Example 3.** Take $K[x]/(P)$, the ring of polynomials in one variable over $K$, modded out by the ideal of an irreducible polynomial $P$. This is a field. Suppose $Q \notin (P)$, then $\gcd(Q, P) = 1$, so for some polynomials $A, B$ we have $AP + BQ = 1$ by Bézout's identity. Hence $BQ \equiv 1 \pmod{P}$, that is, $B$ is an inverse of $Q$ in $K[x]/(P)$.

## 2.2 Algebraic elements. Minimal polynomial.

We continue with the previous example: the quotient $K[x]/(P)$ is a field. Rather than Bézout's identity, we can say that $(P)$ is a **maximal ideal** of $K[x]$, and the quotient of a ring by a maximal ideal is always a field. The proof of this fact uses the same identity.

This field is an extension of $K$ in the obvious way: it is a $K$-algebra!

### 2.2.1 A concrete example.

Let $K = \mathbb{F}_2 = \{0, 1\} = \mathbb{Z}/2\mathbb{Z}$, and $P = x^2 + x + 1$. Then $K[x]/(P)$ contains four elements: 0, 1, the class containing $x$ (denoted by $\bar{x}$, and the class containing $x + 1$ (denoted by $\overline{x+1}$). We have that $\bar{x}^2 = -\bar{x} - 1 = \overline{x+1}$ since $K$ has characteristic 2. Similarly $(\overline{x+1})^2 = \bar{x}$. Moreover, these elements are inverses of each other: $\bar{x}(\overline{x+1}) = \bar{x}^2 + \bar{x} = -1 = 1$. Since $|K[x]/(P)| = 4$, we write $K[x]/(P) = \mathbb{F}_4$. This notation seems presumptuous, implying that there is "only" one field with four elements: in fact every field with a given finite number of elements is isomorphic, so this is true. A proof will come later.

### 2.2.2 Algebraic elements of a field extension.

**Example 4.** Given a field extension $K \subset L$ and an element $\alpha \in L$, we say that $\alpha$ is **algebraic** if there exists some polynomial $P \in K[x]$ such that $P(\alpha) = 0$; if no such polynomial exists, we say that $\alpha$ is **transcendental**.

**Lemma 1.** *If $\alpha$ is algebraic, then there exists a* unique *unitary polynomial $P$ of minimal degree with $P(\alpha) = 0$. $P$ is irreducible, and for any $Q$ such that $Q(\alpha) = 0$, then $Q$ is divisible by $P$.*

**Definition 2.** We call such a polynomial $P$ the **minimal polynomial of $\alpha$ over K**, denoted $P_{\min}(\alpha, K)$.

*Proof of lemma.* We know that $K[x]$ is a **principal ideal domain**, and the polynomials $I = \{Q \in K[x] : Q(\alpha) = 0$ forms an ideal. Thus $I$ has a generator, so $I = (P)$ for some $P$. This generator is a unique (up to a constant) element of minimal degree in $I$. Furthermore, if $P$ was *not* irreducible—if $P = QR$—then $P(\alpha) = Q(\alpha)R(\alpha)$ and so at least one of $Q(\alpha) = 0$ or $R(\alpha) = 0$. This would contradict the minimal-degree condition on $P$. ■

## 2.3 Algebraic elements. Algebraic extensions.

### 2.3.1 An important bit of notation.

**Definition 3.** We denote by $K(\alpha)$ the smallest subfield of $L$ containing $\alpha$. We say that $K[\alpha]$ (note the square braces) is the smallest subring (or $K$-algebra) containing $K$ and $\alpha$.

$K[\alpha]$ is generated, as a vector space over $K$, by $1, \alpha, \alpha^2, \ldots, \alpha^n, \ldots$.

**Example 5.** $\mathbb{C} = \mathbb{R}(\imath)$ as a field, but also $\mathbb{C} = \mathbb{R}[\imath]$ as a ring. Every $z \in \mathbb{C}$ can be written $z = x + \imath y$; this is a vector subspace generated by $1, \imath$.

**Proposition 1.** *The following are equivalent: (1) $\alpha$ is algebraic over $K$; (2) $K[\alpha]$ is a finite dimensional vector space over $K$; (3) $K[\alpha] = K(\alpha)$.*

*Proof.* (1) $\Rightarrow$ (2): We have that $\alpha^d + a_{d-1}\alpha^{d-1} + \ldots + \alpha_1\alpha + a_0 = 0$ for $a_i \in K$ (this is just the minimal polynomial). Then $\alpha^d = -\left(\sum_{k=0}^{d-1} a_k\alpha^k\right)$, a linear combination of the lower powers of $\alpha$. Therefore $K[\alpha]$ is generated by $1, \alpha, \ldots, \alpha^{d-1}$ over $K$: it is finite-dimensional.

(2) $\Rightarrow$ (3): It is enough to prove that $K[\alpha]$ is a field, since $K[\alpha] \subset K(\alpha)$. Let $x \in K[\alpha]$ nonzero. We want to show that $x$ is invertible. Consider the operation of multiplication by $x$, that is, $y \mapsto xy$ for $y \in K[\alpha]$: this is an injective homomorphism of vector spaces over $K$. But as $K[\alpha]$ is finite-dimensional, this is also a surjection, so there exists $z \in K[\alpha]$ such that $xz = 1$. Hence $x$ is invertible, and so $K[\alpha]$ is a field.

(3) $\Rightarrow$ (1): If $\alpha$ is not algebraic, then there exists no polynomial $P$ such that $P(\alpha) = 0$. This means that the natural homomorphism $i : K[x] \to L$ defined by $P \mapsto P(\alpha)$ is injective, but $K[\alpha]$ is *not* a field, and the image of $i$ is a field. Contradiction! ■

### 2.3.2 Definition and properties of algebraic extensions.

**Definition 4.** $L$ is called **algebraic** over $K$ if every element of $L$ is algebraic over $K$.

**Proposition 2.** *If $L$ is algebraic over $K$, then any $K$-subalgebra of $L$ is a field.*

*Proof.* Let $L' \subset L$ be a subalgebra. We know that $\alpha \in L'$ algebraic. Then $K[\alpha] \subset L$ is a field, so $\alpha$ is invertible (when nonzero). This holds for any such (nonzero) $\alpha$, so $L'$ is a field. ∎

**Proposition 3.** *If $K \subset L \subset M$, and $\alpha \in M$ is algebraic over $K$, then $\alpha$ is algebraic over $L$ and its minimal polynomial $P_{\min}(\alpha, L)$ divides $P_{\min}(\alpha, K)$.*

*Proof.* Consider $P_{\min}(\alpha, K)$ as an element of $L[x]$. ∎

## 2.4 Finite extensions. Algebraicity and finiteness.

**Definition 5** (Finite extension)**.** $L$ is said to be a **finite extension** of $K$ if it is a finite-dimensional $K$-vector space. The dimension of $L$ over $K$ is called the **degree** of $L$ over $K$, and is denoted by $[L : K]$.

**Theorem 1.** *Suppose $K \subset L \subset M$. Then $M$ is finite over $K$ if and only if $M$ is finite over $L$ and $L$ is finite over $K$. Moreover, in this case, the degrees multiply: $[M : K] = [M : L][L : K]$.*

*Proof of Thm. 1.* First, suppose $M$ is finite over $K$. Then any linearly independent family $\{m_i\}$ over $L$ are also linearly independent over $K$, so $\dim_L M$ is finite. Now $L$ is a $K$-vector subspace of $M$, so $\dim_K M$ is finite and thus $\dim_K L$ is finite.

Second, let $\{e_i\}_{i=1}^n$ be an $L$-basis of $M$, and $\{\varepsilon_j\}_{j=1}^d$ a $K$-basis of $L$. We want to show that $e_i\varepsilon_j$ form a $K$-basis of $M$. Indeed, for any $x \in M$, we have that $x = \sum_i a_i e_i$ with $a_i \in L$. And for each $i$, $a_i = \sum_j b_{ij}\varepsilon_j$ with $\sum_{i,j} b_{ij}\varepsilon_j \in K$. So we can write $x = \sum_{i,j} b_{ij}\varepsilon_j e_i$, showing that $e_i\varepsilon_j$ generate $M$ over $K$. We now need to verify that these elements are linearly independent over $K$.

If we have $\sum_{i,j} c_{ij}e_i\varepsilon_j = 0$ then $\sum_i \left(\sum_j c_{ij}\varepsilon_j\right) e_i = 0$, and $\sum_j c_{ij}\varepsilon_j \in L$. But $\{e_i\}$ is a basis, so for all $i$, we have $\sum_j c_{ij}\varepsilon_j = 0$. And since $\{\varepsilon_j\}$ is a basis, necessarily $c_{ij} = 0$ for all $i, j$. This proves the theorem. ∎

**Definition 6.** We say that $K(\alpha_1, \ldots, \alpha_n) \subset L$, the smallest subfield of $L$ containing $K, \alpha_1, \ldots, \alpha_n$, is **generated** by $\alpha_1, \ldots, \alpha_n$ over $K$.

**Theorem 2.** *$L$ is finite over $K$ if and only if $L$ is generated by a finite number of algebraic elements over $K$.*

*Proof.* First, suppose that $\{\alpha_i\}_{i=1}^d$ is a $K$-basis of $L$. Then $L = K[\alpha_1, \ldots, \alpha_d] = K(\alpha_1, \ldots, \alpha_d)$. Moreover, each $K[\alpha_i]$ is a finite-dimensional $K$-algebra since it is a subring of (already finite-dimensional) $L$. Then by Proposition 1, $\alpha_i$ is algebraic.

Second, suppose $K[\alpha_1]$ is finite dimensional over $K$; $K[\alpha_1, \alpha_2]$ is finite dimensional over $K[\alpha_1]$; ...; $K[\alpha_1, \dots, \alpha_{d-1}, \alpha_d]$ finite dimensional over $K[\alpha_1, \dots, \alpha_{d-1}]$. Each $\alpha_i$ is algebraic, so for $1 \leq i \leq d$ we have $K[\alpha_1, \dots, \alpha_i] = K(\alpha_1, \dots, \alpha_i)$. Now we use Theorem 1 to conclude that $L = K(\alpha_1, \dots, \alpha_d)$ is finite over $K$. ■

## 2.5 Algebraicity in towers. An example.

Algebraic extensions have a similar property to finite extensions: a tower of extensions is algebraic only if the floor of the tower is algebraic.

**Theorem 3.** *Let $K \subset L \subset M$. Then $M$ is algebraic over $K$ if and only if $M$ is algebraic over $L$ and $L$ is algebraic over $K$.*

*Proof.* First, let $\alpha \in M$. If $P(\alpha) = 0$ for some $P \in K[x]$, then also $P \in L[x]$, so $\alpha$ is algebraic over $L$. Now if $\alpha \in L$ then also $\alpha \in M$ and so $\alpha$ is algebraic over $K$. Thus $L$ is algebraic over $K$.

Second, suppose $L$ is algebraic over $K$ and $M$ is algebraic over $L$; we need to show that $M$ is algebraic over $K$. Take $\alpha \in M$ and consider $P_{\min}(\alpha, L)$. Its coefficients are elements of $L$, so they are algebraic over $K$. By the previous theorem, they generate an extension, $E$, which is *finite* over $K$. Now $E(\alpha)$ is also finite over $K$. Since $E(\alpha)$ is finite over $E$, then $\alpha$ is algebraic over $K$: there exists a linear dependence relation between powers of $\alpha$. ■

We now consider an example.

**Example 6.** Consider $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3})$. This is clearly algebraic and finite over $\mathbb{Q}$. The degree of this extension is 6: we have $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}, \sqrt{3})$. The minimal polynomial $P_{\min}(\sqrt[3]{2}, \mathbb{Q}) = x^3 - 2$; $\mathbb{Q}(\sqrt[3]{2})$ is generated over $\mathbb{Q}$ by $1, \sqrt[3]{2}, (\sqrt[3]{2})^2$, so $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

Now $\sqrt{3} \notin \mathbb{Q}(\sqrt[3]{2})$, because otherwise we would have $\mathbb{Q} \subset \mathbb{Q}(\sqrt{3}) \subset \mathbb{Q}(\sqrt[3]{2})$. Then $2 = [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}]$ would divide $3 = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$, which is impossible. Therefore, $x^2 - 3$ is irreducible over $\mathbb{Q}(\sqrt[3]{2})$, and so is in fact the minimal polynomial for $\sqrt{3}$ over this extension.

The degree of the big extension, $[\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}) : \mathbb{Q}(\sqrt[3]{2})] = 2$, and therefore $[\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}) : \mathbb{Q}] = (2)(3) = 6$.

In fact, this reflects a more general property:

**Proposition 4.** *If $\alpha$ is algebraic over $K$, then the degree of $K(\alpha)$ over $K$ is equal to the degree of the minimal polynomial of $\alpha$ over $K$.*

*Proof.* The proof is obvious: $K(\alpha)$ is generated by the powers of $\alpha$ up to some $\alpha^{d-1}$ (if $\deg P_{\min}(\alpha, K) = d$), and these are linearly independent. ■

This gives us a nice tool to compute the degree of algebraic extensions.

**Proposition 5.** *Let $K \subset L$ be a field extension and let $L' = \{\alpha \in L : \alpha$ is algebraic over $K\}$. Then $L'$ is a subfield of $L$; we call this the **algebraic closure** of $K$ in $L$.*

*Proof.* Let $\alpha, \beta$ be algebraic over $K$. We want to show that $\alpha + \beta$ and $\alpha\beta$ are algebraic; these facts follow immediately from Theorem 2, since $\alpha + \beta$ and $\alpha\beta$ belong to $K[\alpha, \beta]$, which is a finite (by Theorem 2) extension of $K$. ■

## 2.6 A digression: Gauss lemma, Eisenstein criterion.

### 2.6.1 A brief review.

We said that for a field $K$, an element $\alpha$ is algebraic over $K$ if $\alpha$ is a root of some polynomial $P \in K[x]$.

We said that an extension $L$ is algebraic over $K$ if every element $\alpha \in L$ is algebraic over $K$.

We said that $L$ is finite over $K$ if the dimension of $L$ over $K$ is finite.

We saw that finite implies algebraic, and that we have finiteness if and only if the field is algebraic *and* finitely generated.

Finally, we deduced that $[K(\alpha) : K] = \deg P_{\min}(\alpha, K)$.

Therefore, it's important to be able to know whether a given polynomial is in fact irreducible over $K$.

### 2.6.2 How to decide that a polynomial is irreducible over K.

In our example we had $x^3 - 2$ is irreducible $\mathbb{Q}$. Since the degree of this polynomial is equal to 3 and there is no root in $\mathbb{Q}$.

But if we ask whether $x^{100} - 2$ is irreducible over $\mathbb{Q}$, this is not so trivial. In fact it is irreducible, based on a few facts.

**Lemma 2** (Gauss)**.** *Let $P \in \mathbb{Z}[x]$. If $P$ decomposes nontrivially (that is, $P = QR$, where $\deg Q, \deg R < \deg P$) over $\mathbb{Q}$, then it also decomposes over $\mathbb{Z}$.*

*Proof.* Let $P = QR$. Set $mQ = Q_1 \in \mathbb{Z}[x]$ and $nR = R_1 \in \mathbb{Z}[x]$. Then $mnP = Q_1R_1 \in \mathbb{Z}[x]$. For $p|mn$, then modulo $p$ we have $0 = \bar{Q}_1\bar{R}_1$. Since we're working over $\mathbb{F}_p$ a field, we have that $\bar{Q}_1 = 0 \pmod{p}$ or $\bar{R}_1 = 0 \pmod{p}$: that is, $p$ divides all of the coefficients of either $Q_1$ or $R_1$. WLOG say this is $Q_1$. Then $\frac{mn}{p}P = Q_2R_1 \in \mathbb{Z}[x]$ where $Q_2 = \frac{Q_1}{p}$. Continuing in this way, we arrive at $P = Q_lR_s \in \mathbb{Z}[x]$. ∎

**Example 7** (Eisenstein criterion example)**.** To show that $x^{100} - 2$ is irreducible over $\mathbb{Z}$? We reduce modulo 2: if $x^{100} - 2 = QR$ then $x^{100} = \bar{Q}\bar{R}$ in $\mathbb{F}_2[x]$, so $\bar{Q}$ and $\bar{R}$ are of the form $x^k$ respectively $x^l$. The constant coefficients of both $\bar{Q}$ and $\bar{R}$ must be divisible by 2; hence the constant coefficient of $x^{100} - 2$ must be divisible by 4, except this is not the case. Therefore

**Proposition 6** (Eistenstein criterion)**.** *Let $P \in \mathbb{Z}[x]$ with $P = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$. If there exists a prime $p$ such that (1) $p$ divides $a_n$; (2) $p$ divides $a_i$ for $i = 0, \ldots, n-1$; and (3) $p^2$ does not divide $a_0$; then $P \in \mathbb{Z}[x]$ is irreducible.*

*Proof.* The proof is the same as in the example. ∎

Both facts are valid in more generality, by replacing $\mathbb{Z}$ with any unique factorization domain $R$, and replacing $\mathbb{Q}$ by the fraction field of $R$.

# Quiz 1

### Which of the following are true?

*Solution.* **A finite extension of fields is algebraic.** This is *true.*

**An algebraic extension of fields is finite.** This is *false*; for example, the field of all algebraic numbers is an infinite extension of $\mathbb{Q}$.

**A finitely generated and algebraic extension of fields is finite.** This is *true.* ■

### Which of the following pairs is an extension of fields?

*Solution.* $\mathbb{Z}, \mathbb{Q}$ is *not* a field extension because $\mathbb{Z}$ is not a field.

$\mathbb{Q}, \mathbb{R}$ is a field extension because $\mathbb{R}$ is a field and $\mathbb{Q} \subset \mathbb{R}$.

$\mathbb{Q}(\imath), \mathbb{R}$ is *not* a field extension because, e.g., $\imath \in \mathbb{Q}(\imath)$ but $\imath \notin \mathbb{R}$, and so $\mathbb{Q}(\imath)$ is not a subfield of $\mathbb{R}$.

$\mathbb{Q}(\imath), \mathbb{C}$ is a field extension because $\mathbb{C}$ is a field and $\mathbb{Q}(\imath) \subset \mathbb{C}$. ■

### What is the minimal polynomial of $e^{2\pi\imath/3}$ over $\mathbb{Q}$?

*Solution.* Let $\zeta = e^{2\pi\imath/3}$, and note that $\zeta^3 = e^{2\pi\imath} = 1$. Therefore $\zeta$ is a root of the polynomial $Q(x) = x^3 - 1$. Now $Q$ is not irreducible: $Q = PR$, where $P(x) = x^2 + x + 1$ and $R(x) = x - 1$. $R(\zeta) \neq 0$ but $P(\zeta) = 0$, and $P$ is irreducible over $Q$ (by, e.g., the quadratic formula). Therefore $P(x) = x^2 + x + 1$ is the minimal polynomial for $\zeta$ over $\mathbb{Q}$. ■

Which of the following polynomials $f$ is irreducible over the specified field $K$?

*Solution.* $f_1 = x^2 + x + 1$ is irreducible over $K_1 = \mathbb{Q}$; see previous question.

$f_2 = x^2 - 2$ is irreducible over $K_2 = \mathbb{Q}$, since its roots are $\pm\sqrt{2} \notin \mathbb{Q}$.

$f_3 = x^2 - 2$ is *not* irreducible over $K_3 = \mathbb{R}$, since its roots are $\pm\sqrt{2} \in \mathbb{R}$.

$f_4 = x^2 + x + 1$ is *not* irreducible over $K_4 = \mathbb{F}_3$: we have $f_4(1) = 1 + 1 + 1 = 0$ since the field has characteristic 3, and $1 \in \mathbb{F}_3$.

$f_5 = x^4 + 6x^2 + 2$ is irreducible over $K_5 = \mathbb{Q}$. Setting $y = x^2$ and $\hat{f}_5 = y^2 + 6y + 2$, we obtain by the quadratic formula

$$y = \frac{-6 \pm \sqrt{36-4}}{2} = \frac{-6 \pm \sqrt{32}}{2} = \frac{-6 \pm 4\sqrt{2}}{2} = -3 \pm 2\sqrt{2},$$

and hence $x = \pm\sqrt{-3 \pm 2\sqrt{2}} \notin \mathbb{Q}$.

$f_6 = x^3 - 1$ is *not* irreducible over $K_6 = \mathbb{Q}$; see previous question. ■

**Which of the following quotient rings is a field?**

*Solution.* Note that this is equivalent to asking if the polynomial we're modding out by is irreducible over the base field.

$\mathbb{R}[x]/(x^2-2)$ is *not* a field, since $x^2-2$ is not irreducible over $\mathbb{R}$.

$\mathbb{Q}[x]/(x^2-2)$ is a field, since $x^2-2$ is irreducible over $\mathbb{Q}$.

$\mathbb{F}_3[x]/(x^2+x+1)$ is *not* a field, since $x^2+x+1$ is not irreducible over $F_3$.

$\mathbb{R}[x]/(x^2-1)$ is *not* a field, since $x^2-1$ is not irreducible over $\mathbb{R}$.

$\mathbb{R}[x]/(x^2+1)$ is a field, since $x^2+1$ is irreducible over $\mathbb{R}$. ■

**What is the degree of the field extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$?**

*Solution.* We know that the extension is generated by products of $1, \sqrt{2}, \sqrt{3}$. Now $1^2 = 1$, $(\sqrt{3})^2 = 3$, $(\sqrt{2})^2 = 2$, and $\sqrt{2}\sqrt{3} = \sqrt{6}$; therefore any element $q \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ can be written $q = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ with $a, b, c, d \in \mathbb{Q}$. Therefore $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$. ■