Solutions to David A.Cox "Galois Theory"

Richard Ganaye

October 10, 2021

3 Chapter 3

3.1 THE EXISTENCE OF ROOTS

Ex. 3.1.1 *This exercise is concerned with the proof of Proposition 3.1.1. Suppose that $f, g, h \in F[x]$ are polynomials such that f is nonzero and $f = gh$. Also let $I = \langle g \rangle$.*

(a) Prove that g constant if and only if $I = F[x]$.

(b) Prove that h constant if and only if $I = \langle f \rangle$.

Proof. Let $f, g, h \in F[x], f \neq 0, f = gh, I = \langle g \rangle$.

(a) • Suppose that $g = \lambda \in F$ is a constant. As $f \neq 0$ and $f = gh$, then $g \neq 0$, so $\lambda \neq 0$.

Let $p \in F[x]$ any polynomial. Then $p = \lambda(\frac{1}{\lambda}p) = (\frac{1}{\lambda}p)g \in \langle g \rangle$, thus $F[x] \subset \langle g \rangle$. Moreover $\langle g \rangle \subset F[x]$, so

$$F[x] = \langle g \rangle = I.$$

• Conversely, if $F[x] = I = \langle g \rangle$, then $1 \in \langle g \rangle$, so $1 = gu, u \in F[x]$, hence $0 = \deg(g) + \deg(u)$, therefore $\deg(g) = 0$, so $g \in F$ is a nonzero constant.

$$g \in F^* \iff \langle g \rangle = F[x].$$

(b) • If $h = \mu \in F$ is a constant, then $\mu \neq 0$ (since $f \neq 0$), and $f = \mu g, \mu \in F^*$.

If $p \in \langle f \rangle$, then $p = uf, u \in F[x]$, thus $p = \mu u g \in \langle g \rangle$, so $\langle f \rangle \subset \langle g \rangle$.

If $p \in \langle g \rangle$, then $p = qg, q \in F[x]$, thus $p = \mu^{-1} q f \in \langle f \rangle$, so $\langle g \rangle \subset \langle f \rangle$.

$$\langle f \rangle = \langle g \rangle = I.$$

• Conversely, if $\langle f \rangle = \langle g \rangle$, then $g \in \langle f \rangle$, $g = vf, v \in k[x]$, thus $g = vgh$. As $f = gh \neq 0, g \neq 0$, thus $1 = vh$, therefore $h \in F^*$ is a constant.

$$h \in F^* \iff I = \langle f \rangle.$$

□

Ex. 3.1.2 *Let F and L be fields, and let $\varphi : F \to L$ be a ring homomorphism. Prove that φ is one-to-one and that we get an isomorphism $\varphi : F \simeq \varphi(F)$.*

Proof. Let $x \in F$. If $x \neq 0$, then $x.x^{-1} = 1$, thus $\varphi(x)\varphi(x^{-1}) = 1$, so $\varphi(x) \neq 0$. For all $x \in F$, $x \neq 0 \Rightarrow \varphi(x) \neq 0$, therefore $\varphi(x) = 0 \Rightarrow x = 0$, so $\ker(\varphi) = \{0\}$ and φ is injective.

Consequently, the corestriction $F \to \varphi(F), x \mapsto \varphi(x)$ is a bijection, so it is a ring isomorphism $\varphi : F \simeq \varphi(F)$. □

Ex. 3.1.3 *Let $I \subset F[x]$ be an ideal, and define $\varphi : F \to F[x]/I$ by $\varphi(a) = a + I$. Prove carefully that φ is a ring homomorphism.*

Proof. Let $a, b \in A = F[x]$. Suppose that $a + I = a' + I$ et $b + I = b' + I$.

Then $a' = a + u, u \in I, b' = b + v, v \in I$, so $a' + b' = a + b + u + v$, where $u + v \in I$, thus $a + b + I = a' + b' + I$.

$a'b' = ab + bu + av + uv$, where $bu + av + uv \in I$, so $ab + I = a'b' + I$.

The equivalence relation $\sim$ defined on A as $a \sim a' \iff a+I = a'+I (\iff a'-a \in I)$ is so compatible with addition and multiplication in A, and the class of an element $a \in A$ is $a + I$. We can so define sum and product of two classes by

$$(a + I) + (b + I) = a + b + I, \tag{1}$$
$$(a + I)(b + I) = ab + I. \tag{2}$$

If $\varphi : A \to A/I$ is defined by $\varphi(a) = a + I$, then (1) and (2) are written

$$\varphi(a) + \varphi(b) = \varphi(a + b), \varphi(a)\varphi(b) = \varphi(ab)$$

Moreover $\varphi(1) = 1 + I$ is the multiplicative identity of A/I.

$\varphi : A \to A/I$ is a ring homomorphism. □

Ex. 3.1.4 *In your abstract algebra text, review the definition of the field of fractions of an integral domain and verify that (3.3) is the correct definition of a/b for $a, b \in \mathbb{Z}, b \neq 0$.*

Proof. The relation $\sim$ on $\mathbb{Z} \times \mathbb{Z}^*$ defined by

$$(a, b) \sim (c, d) \iff ad = bc$$

is an equivalence relation. The class of (a, b), written $\frac{a}{b}$ is so the set

$$\frac{a}{b} = \{(c, d) \in \mathbb{Z} \times \mathbb{Z}^* \mid ad = bc\}.$$

□

Ex. 3.1.5 *Let $f \in F[x]$ be irreducible, and let $g+\langle f\rangle$ be a nonzero coset in the quotient ring $L = F[x]/\langle f\rangle$.*

(a) Show that f and g are relatively prime and conclude that $Af + Bg = 1$, where A, B are polynomials in $F[x]$.

(b) Show that $B + \langle f\rangle$ is the multiplicative inverse of $g + \langle f\rangle$ in L.

Proof. Let $f \in F[x]$ be irreducible, and let $L = F[x]/\langle f\rangle$ the quotient ring.

(a) Let $\overline{g} \in L, \overline{g} \neq \overline{0}$, that is to say $g + \langle f \rangle \neq 0 + \langle f \rangle$, which is equivalent to $g \notin \langle f \rangle$, or $f \nmid g$ (in $F[x]$).

Let h a common divisor of f et g. Since f is irreducible, either u is a nonzero constant, or $u = kf, k \in F^*$ is associate to f. But in this last case, $f = k^{-1}u$ divides u, which divides g, so $f \mid g$, in contradiction with the hypothesis.

So the only common divisors of f, g are the nonzero constants, thus $f \wedge g = 1$.

By Bézout theorem, there exist polynomials $A, B \in k[x]$ such that

$$1 = Af + Bg.$$

(b) As $\overline{f} = f + \langle f \rangle = \overline{0}$, $\overline{1} = \overline{A}\,\overline{f} + \overline{B}\overline{g} = \overline{B}\overline{g}$, which we can write

$$1 + \langle f \rangle = (B + \langle f \rangle)(g + \langle f \rangle).$$

So $B + \langle f \rangle$ is the inverse of $g + \langle f \rangle$ in $L = F[x]/\langle f \rangle$.

□

Ex. 3.1.6 *Apply the method of Exercise 5 to find the multiplicative inverse of the coset $1 + x + \langle x^2 + x + 1 \rangle$ in the field $\mathbb{Q}[x]/\langle x^2 + x + 1 \rangle$.*

Proof. $f = x^2 + x + 1$ has no root in $\mathbb{Q}$ is has degree 2, therefore f is irreducible on $\mathbb{Q}$, and consequently $\mathbb{Q}[x]/\langle f \rangle$ is a field.

Moreover $-x(x + 1) + (x^2 + x + 1) = 1$ is a Bézout's relation between $x + 1$ and $x^2 + x + 1$. This gives the following equality in $\mathbb{Q}[x]/\langle f \rangle$:

$$(-x + \langle f \rangle)(x + 1 + \langle f \rangle) + (x^2 + x + 1) + \langle f \rangle = 1 + \langle f \rangle,$$

so

$$(-x + \langle f \rangle)(x + 1 + \langle f \rangle) = 1 + \langle f \rangle.$$

$-x + \langle f \rangle$ is the inverse of $x + 1 + \langle f \rangle$ in $\mathbb{Q}[x]/\langle f \rangle$. □

3.2 THE FUNDAMENTAL THEOREM OF ALGEBRA

Ex. 3.2.1 *For $f \in \mathbb{C}[x]$, define $\overline{f}$ as in (3.5).*

(a) Show carefully that $\overline{fg} = \overline{f}\,\overline{g}$ for $f, g \in \mathbb{C}[x]$.

(b) Let $\alpha \in \mathbb{C}$. Show that $\overline{f}(\alpha) = 0$ implies that $f(\overline{\alpha}) = 0$.

Proof. (a) Let $f = \sum_{i=0}^{n} a_i x^i, g = \sum_{j=0}^{m} b_j x^i \in \mathbb{C}[x]$.

By definition of the product of polynomials,

$$fg = \sum_{k=0}^{n+m} c_k x^k, \text{ with } c_k = \sum_{i+j=k} a_i b_j = \sum_{i=0}^{k} a_i b_{k-i}$$

Then, using the fact that conjugation is a field automorphism in $\mathbb{C}$,

$$\begin{aligned}
\overline{fg} &= \sum_{k=0}^{n+m} \overline{c_k} x^k \\
&= \sum_{k=0}^{n+m} \overline{\sum_{i+j=k} a_i b_j} x^k \\
&= \sum_{k=0}^{n+m} \sum_{i+j=k} \overline{a_i}\,\overline{b_j} x^k \\
&= \sum_{i=0}^{n} \overline{a_i} x^i \sum_{j=0}^{n} \overline{b_j} x^j \\
&= \overline{f}\,\overline{g}.
\end{aligned}$$

(b) If $f \in \mathbb{C}[x]$ and $\alpha \in \mathbb{C}$,

$$\begin{aligned}
\overline{f}(\alpha) = 0 &\Rightarrow \sum_{i=0}^{n} \overline{a_i} \alpha^i = 0 \\
&\Rightarrow \overline{\sum_{i=0}^{n} \overline{a_i} \alpha^i} = \overline{0} = 0 \\
&\Rightarrow \sum_{i=0}^{n} a_i \overline{\alpha}^i = 0 \\
&\Rightarrow f(\overline{\alpha}) = 0.
\end{aligned}$$

□

Ex. 3.2.2 *In Section A.2, we use polar coordinates to construct square (and higher) roots of complex numbers. In this exercise, you will give an elementary argument that every complex number has a square root. The only fact you will use (besides standard algebra) is that every positive real number has a real square root.*

(a) *First explain why every real number has a square root in $\mathbb{C}$.*

(b) *Now fix $a+bi \in \mathbb{C}$ with $b \neq 0$. For $x, y \in \mathbb{R}$, show that the equation $(x+iy)^2 = a+bi$ is equivalent to the equations*

$$x^2 - y^2 = a, \qquad 2xy = b.$$

(c) *Show that the equation of part (b) are equivalent to*

$$x^2 = \frac{a \pm \sqrt{a^2+b^2}}{2}, \qquad y = \frac{b}{2x}.$$

Also show that $x \neq 0$ and that $a \pm \sqrt{a^2+b^2}$ is positive when we choose the + sign in the formula for x^2.

(d) *Conclude that $a+bi$ has a square root in $\mathbb{C}$.*

Proof. (a) We know that the equation $x^2 = a$ has a real solution if $a \geq 0$ (see Ex. 3.2.3). Therefore, if $a \in \mathbb{R}_*^-$, there exists $b \in \mathbb{R}^+$ such that $b^2 = -a = |a|$. Thus $(ib)^2 = a$.

Conclusion: Every $a \in \mathbb{R}$ has a square root in $\mathbb{C}$.

(b,c,d) Let $z = a + ib,\ a, b \in \mathbb{R}$, and $Z = x + iy,\ x, y \in \mathbb{R}$ two complex numbers.

$$\begin{aligned} z^2 = Z &\iff (a+ib)^2 = x + iy \\ &\iff (a+ib)^2 = x+iy \text{ and } |a+ib|^2 = |x+iy| \\ &\iff a^2 - b^2 + 2abi = x + iy \text{ and } a^2 + b^2 = \sqrt{x^2+y^2} \\ &\iff a^2 - b^2 = x, a^2 + b^2 = \sqrt{x^2+y^2}, 2ab = y. \end{aligned}$$

The system of equations $\begin{cases} a^2 - b^2 &= & x, \\ a^2 + b^2 &= & \sqrt{x^2+y^2}, \end{cases}$ is equivalent to

$$\begin{cases} a^2 &= \frac{1}{2}\left(\sqrt{x^2+y^2} + x\right), \\ b^2 &= \frac{1}{2}\left(\sqrt{x^2+y^2} - x\right). \end{cases}$$

Therefore

$$z^2 = Z \Rightarrow \begin{cases} a^2 &= \frac{1}{2}\left(\sqrt{x^2+y^2} + x\right), \\ b^2 &= \frac{1}{2}\left(\sqrt{x^2+y^2} - x\right), \\ \operatorname{sgn}(ab) &= \operatorname{sgn}(y). \end{cases}$$

The converse is true, since these last equations imply

$$4a^2b^2 = \left(\sqrt{x^2+y^2} + x\right)\left(\sqrt{x^2+y^2} - x\right) = x^2 + y^2 - x^2 = y^2,$$

and since $\operatorname{sgn}(ab) = \operatorname{sgn}(y)$, we conclude $2ab = y$. So we have proved the equivalence

$$z^2 = Z \iff \begin{cases} a^2 &= \frac{1}{2}\left(\sqrt{x^2+y^2} + x\right), \\ b^2 &= \frac{1}{2}\left(\sqrt{x^2+y^2} - x\right), \\ \operatorname{sgn}(ab) &= \operatorname{sgn}(y). \end{cases}$$

As $x^2 + y^2 \geq x^2$, $\sqrt{x^2+y^2} \geq |x|$, and $|x| \geq x, |x| \geq -x$, so

$$\begin{aligned} z^2 = Z &\iff \begin{cases} a &= \varepsilon\sqrt{\frac{1}{2}\left(\sqrt{x^2+y^2} + x\right)} \\ b &= \varepsilon \operatorname{sgn}(y)\sqrt{\frac{1}{2}\left(\sqrt{x^2+y^2} - x\right)}, \end{cases} \qquad \varepsilon \in \{-1, 1\} \\ &\iff z \in \{z_0, -z_0\}, \end{aligned}$$

where

$$z_0 = \sqrt{\frac{1}{2}\left(\sqrt{x^2+y^2} + x\right)} + i \operatorname{sgn}(y)\sqrt{\frac{1}{2}\left(\sqrt{x^2+y^2} - x\right)}.$$

Conclusion: Every $z \in \mathbb{C}$ has a square root in $\mathbb{C}$.

□

Ex. 3.2.3 *Use the IVT to prove that every positive real number a has a real square root.*

Proof. Suppose that $a \in \mathbb{R}^+$.

Let $u : \mathbb{R} \to \mathbb{R}$ defined by $x \mapsto u(x) = x^2 - a$.

Then u is continuous, u is strictly increasing, and

$u(0) = -a \le 0$, $\lim\limits_{x\to\infty} u(x) = +\infty$ (so there exists $A \in \mathbb{R}^+$ such that $u(A) > 0$).

By the Intermediate Value Theorem, there exists a unique $b \in \mathbb{R}^+$ such that $b^2 = a$, so a has a real square root. $\square$

Ex. 3.2.4 *A field F is an ordered field if there is a subset $P \subset F$ such that:*

(a) P is closed under addition and multiplication.

(b) For any $a \in F$, exactly one of the following is true: $a \in P, a = 0$, or $-a \in P$.

One then defines $a > b$ to mean $a-b \in P$ (so that P becomes the set of positive elements). From this, one can prove all the typical properties of $>$. Now let F be an ordered field. Prove that -1 is not a square in F.

Proof. Let F an ordered field.

Since P is closed under multiplication by (a), if $a \in P$, then $a^2 \in P$.

If $-a \in P$, $a^2 = (-a)(-a) \in P$. By (b), every $a \in F$ verifies $a \in P$, or $a = 0$, or $-a \in P$, so we can conclude that

$$\forall a,\ a \in F^* \Rightarrow\ a^2 \in P. \tag{3}$$

So P contains all squares in F, 0 excluded. By definition of fields, we know that $1 \neq 0$, so $1 = 1^2 \in P$.

By (b), the three cases $a \in P$, $a = 0$, $-a \in P$ are mutually exclusive, thus $-1 \notin P$. Therefore -1 is not a square in F, otherwise $-1 = a^2 \in P$ by (3).

Conclusion: -1 is not a square in the ordered field F. $\square$

Ex. 3.2.5 *Let F be a real closed field. As in the text, this means that F is an ordered field (see Exercise 4) such that every positive element of F has a square root in F and every $f \in F[x]$ of odd degree has a root in F.*

(a) Use Exercise 4 to show that x^2+1 is irreducible over F. Then define $F(i)$ to be the field $F[x]/\langle x^2+1\rangle$. By the Cauchy construction described in Section 3.1, elements of $F(i)$ can be written $a+bi$ for $a, b \in F$.

(b) Show that every quadratic polynomial in $F(i)$ splits completely over $F(i)$.

(c) Prove that $F(i)$ is algebraically closed.

Proof. (a) Since -1 is not a square in F by Exercise 4, the polynomial x^2+1 has no root in F, and it has degree 2, thus it is irreducible over F.

Therefore $F(i) = F[x]/\langle x^2+1\rangle$ is a field, where $i = x + \langle x^2+1\rangle$, by Proposition 3.1.1.

The division of any polynomial f by x^2+1 gives

$$f = q(x^2+1) + bx + a,$$

so every $y \in F(i)$ is of the form $y = a + ib$.

(b) Let $ax^2 + bx + c,\ a, b, c \in F(i), a \neq 0$, any quadratic polynomial.

$$\begin{aligned} ax^2 + bx + c &= a\left(x^2 + \frac{b}{a}x + \frac{c}{a}\right) \\ &= a\left[\left(x + \frac{b}{2a}\right)^2 - \frac{b^2}{4a^2} + \frac{c}{a}\right] \\ &= a\left[\left(x + \frac{b}{2a}\right)^2 - \frac{\Delta}{4a^2}\right], \Delta = b^2 - 4ac \end{aligned}$$

By definition of a real closed field, every positive element of F has a square root in F. With the same proof as in Ex 3.2.2, we can prove that every $z \in F(i)$ has a square root. One square root of $z = x + iy,\ x, y \in F$, is given by

$$z_0 = \sqrt{\frac{1}{2}\left(\sqrt{x^2+y^2} + x\right)} + i \ \mathrm{sgn}(y)\sqrt{\frac{1}{2}\left(\sqrt{x^2+y^2} - x\right)}.$$

We will write $\sqrt{\Delta}$ one of the square roots of Δ. Then

$$\begin{aligned} ax^2 + bx + c &= a\left[\left(x + \frac{b}{2a}\right)^2 - \left(\frac{\sqrt{\Delta}}{2a}\right)^2\right] \\ &= a(x - x_1)(x - x_2), x_1 = \frac{-b + \sqrt{\Delta}}{2} \in F(i), x_2 = \frac{-b + \sqrt{\Delta}}{2} \in F(i) \end{aligned}$$

splits completely over $F(i)$.

(c) By definition of a real closed field, and by (b),

- every polynomial of odd degree in $F[x]$ has a root in F,
- every element $a \in F(i)$ has a square root in $F(i)$,
- every quadratic polynomial $f \in F(i)[x]$ splits completely over $F(i)$.

The Proposition 3.2.2 and the Lemme 3.2.3 are so satisfied if we replace $\mathbb{R}$ by F and $\mathbb{C}$ by $F(i)$.

Theorem 3.2.4 for $F(i)$ follows, with the same proof: $F(i)$ is an algebraically closed field.

$\square$

Ex. 3.2.6 *Here is yet another way to state the Fundamental Theorem of Algebra.*

(a) Suppose that $f(\alpha) = 0$, where $f \in \mathbb{R}[x]$ and $\alpha \in \mathbb{C}$. Prove that $f(\overline{\alpha}) = 0$.

(b) Prove that the Fundamental Theorem of Algebra is equivalent to the assertion that every nonconstant polynomial in $\mathbb{R}[x]$ is a product of linear and quadratic factors with real coefficients.

Proof. (a) Let $f \in \mathbb{R}[x]$, and suppose that $f(\alpha) = 0$. Then $\overline{f} = f$, and $\overline{f}(\alpha) = 0$. By Ex. 3.3.1(b), this implies $f(\overline{\alpha}) = 0$.

Conclusion : if $f \in \mathbb{R}[x]$,

$$f(\alpha) = 0 \Rightarrow f(\overline{\alpha}) = 0.$$

(b) • Suppose that every nonconstant polynomial in $\mathbb{C}[x]$ has a root in $\mathbb{C}$.

Name $x_1, \cdots, x_r$ the real roots of f : $f = a(x-x_1)^{k_1} \cdots (x-x_r)^{k_r} g$, where $a \in \mathbb{R}$, and $g \in \mathbb{R}[x]$ is monic and has no real root. We show by induction on d that every polynomial $g \in \mathbb{R}[x]$ without real root, monic, of degree d, is product of monic quadratic real polynomials.

If $d = 0$, $g = 1$ is the empty product.

We suppose $d > 0$, and put the induction hypothesis that every polynomial in $\mathbb{R}[x]$ without real root, monic, of degree less than d, is product of monic quadratic real polynomials.

Let $g \in \mathbb{R}[x]$ a polynomial of degree d without real root. g has by hypothesis a complex root α. Then $g = (x-\alpha)g_1, g_1 \in \mathbb{C}[X]$.

By (a), $\overline{\alpha}$ is a root of g. $0 = g(\overline{\alpha}) = (\overline{\alpha} - \alpha)g_1(\alpha)$, and $\overline{\alpha} \neq \alpha$, thus $g_1(\overline{\alpha}) = 0$, $g_1 = (x - \overline{\alpha})h, h \in \mathbb{C}[x]$, therefore

$$g = (x-\alpha)(x-\overline{\alpha})h, \ h \in \mathbb{C}[x].$$

$u = (x-\alpha)(x-\overline{\alpha}) = x^2 + sx + t$, where $s = \alpha + \overline{\alpha} \in \mathbb{R}, t = \alpha\overline{\alpha} \in \mathbb{R}$, thus $u \in \mathbb{R}[x]$, and also $h \in \mathbb{R}[x]$, since h is the quotient of the Euclidean division of g by u.

$g = (x^2 - sx + t)h$, where $h \in \mathbb{R}[x]$ is monic, of degree less than d, without real root. By the induction hypothesis, h is product of monic real quadratic polynomials, thus it is the same for g, and the induction is done.

Consequently, f is product of linear or quadratic factors with real coefficients.

• Conversely, suppose that every polynomial in $\mathbb{R}[x]$ is product of linear or quadratic factors with real coefficients.

Let $f \in \mathbb{C}[x]$, with $\deg(f) \geq 1$. We will show that f has a complex root.

By hypothesis f has a linear or a quadratic factor.

If f has a linear factor $ax+b$, then $-b/a$ is a (real) root of f, and if f has a factor ax^2+bx+c, $a \neq 0$, then Lemma 3.2.3 and Exercise 3.2.2 show that f has a complex root. In both cases, f has a complex root, so every non constant polynomial in $\mathbb{C}[x]$ has a complex root.

□

Ex. 3.2.7 *Prove that a field F is algebraically closed if and only if every nonconstant polynomial in $F[x]$ has a root in F.*

Proof. By definition, a field F is algebraically closed if every nonconstant polynomial is product of linear factors in $F[x]$.

• If F is algebraically closed, and if $f \in F[x]$ is not a constant, this product of linear factors is not empty, so f is divisible by a linear factor $ax+b, a, b \in F$. Hence f has a root $\alpha = -b/a$ in F.

• Suppose that every nonconstant polynomial has a root in F

We show by induction on d that every polynomial $f \in F[x], d = \deg(f) > 0$ is product of linear factors in $F[x]$

If $d = 1$, $f = ax + b$, $a \neq 0$, is product of one linear factor.

Let $f \in F[x], d = \deg(f) > 1$. Then f has by hypothesis a root $\alpha \in F$, so $f = (x-a)g$, where $\deg(g) < d$. By the induction hypothesis, g is a constant or is product of linear factors, so it is the same for f, and the induction is done.

Conclusion: If F is a field, the two following propositions are equivalent,

(i) Every nonconstant polynomial in $F[x]$ is product of linear factors.

(ii) Every nonconstant polynomial in $F[x]$ has a root in F

□