III.K. Gauss's lemma and polynomials over UFDs

Let R be a UFD, and $F := \mathfrak{F}(R)$ its field of fractions. Recall that $R[x]^* = R^*$ and $F[x]^* = F^* = F\backslash\{0\}$.

III.K.1. DEFINITION. (i) Given $f = \sum_{k=0}^{n} a_k x^k \in R[x]$, the **content of f** (defined up to units) is $c(f) := \gcd(\{a_k\}) \in R$.

(ii) f is **primitive** if $c(f) \sim 1$. Notice that monic polynomials are primitive.

Clearly in general $f = c(f) \cdot g$, with g primitive, since

$$c(f) = \gcd(\{a_k\}) = c(f) \cdot \gcd(\{\tfrac{a_k}{c(f)}\}) \quad \Longrightarrow \quad \gcd(\{\tfrac{a_k}{c(f)}\}) = 1.$$

III.K.2. PROPOSITION. *Given $f \in F[x]\backslash\{0\}$, we have*

$$f = \alpha g, \quad \text{with } \begin{cases} g \in R[x] \text{ primitive} \\ \alpha \in F^* \end{cases}, \tag{III.K.3}$$

in which g is unique up to multiplication by units (i.e. R^*).

III.K.4. REMARK. One way we will apply this is via

$$\begin{cases} f = \alpha g \\ f, g \text{ both primitive} \in R[x] \\ \alpha \in F^* \end{cases} \quad \Longrightarrow \quad \alpha \in R^*. \tag{III.K.5}$$

This follows from III.K.2 since $1 \cdot f = f = \alpha \cdot g$ gives two decompositions of the form (III.K.3), so that the uniqueness implies that $f = g \cdot \text{unit}$. More loosely, (III.K.5) says that "two primitive polynomials which are associate in $F[x]$ are associate in $R[x]$."

PROOF OF III.K.2. Write $f = \sum_{k=0}^{n} \frac{a_k}{b_k} x^k$, $a_k \in R$, $b_k \in R\backslash\{0\}$. Let $\beta := \prod_k b_k$, so that $\beta f \in R[x]$, and $\gamma := c(\beta f)$. Then $g := \frac{\beta}{\gamma} f \in R[x]$ is primitive and $f = \frac{\gamma}{\beta} g$. If $\alpha' g' = f = \alpha g$ with g, g' primitive, then

$\exists b \in R$ such that

$$\begin{aligned} \alpha b, \alpha' b \in R \quad &\Longrightarrow \quad \underbrace{(\alpha b) g}_{\text{content } \alpha b} = \underbrace{(\alpha' b) g'}_{\text{content } \alpha' b} \\ &\Longrightarrow \quad \alpha b \sim \alpha' b \\ &\Longrightarrow \quad u\alpha b = \alpha' b \quad (u \in R^*) \\ &\Longrightarrow \quad \alpha b g = u \alpha b g' \\ &\Longrightarrow \quad g = u g' \\ &\Longrightarrow \quad g \sim g', \end{aligned}$$

which completes the proof. □

The following basic result goes back to Gauss's Disquisitiones Arithmeticae (c. 1800).

III.K.6. GAUSS'S LEMMA (v. 1.0). *$f, g \in R[x]$ primitive $\Longrightarrow$ fg primitive.*

PROOF. Write $f = \sum_{i=0}^{n} a_i x^i$, $g = \sum_{j=0}^{m} b_j x^j$, $fg = \sum_{k=0}^{m+n} c_k x^k$, and *suppose that* $c(fg) \notin R^*$ (aiming for a contradiction). Let $r \mid c(fg)$ be irreducible. Since R is a UFD, r is also prime.

As f [resp. g] is primitive, r cannot divide all the a_i [resp. b_j], and so there exists a *least* i_0 [resp. j_0] such that $r \nmid a_{i_0}$ [resp. $r \nmid b_{j_0}$]. Since r is prime, we have $r \nmid a_{i_0} b_{j_0}$. On the other hand, $r \mid \sum_{\ell < i_0} a_\ell b_{i_0+j_0-\ell}$ and $r \mid \sum_{\ell > i_0} a_\ell b_{i_0+j_0-\ell}$, so that

$$r \nmid \left(\textstyle\sum_{\ell < i_0} a_\ell b_{i_0+j_0-\ell} + a_{i_0} b_{j_0} + \sum_{\ell > i_0} a_\ell b_{i_0+j_0-\ell} \right) = c_{i_0+j_0}.$$

This contradicts the assumption that r divides $c(fg)$. Conclude that $c(fg) \in R^*$ and fg is primitive. □

Now let $h \in R[x] \backslash R$ be a polynomial of positive degree.

III.K.7. GAUSS'S LEMMA (v. 2.0). *h is irreducible in $R[x]$ $\Longleftrightarrow$ h is primitive (in $R[x]$) and irreducible in $F[x]$.*

PROOF. ($\Longleftarrow$): If h is reducible in $R[x]$, then we have $h = fg$ with $f, g \notin R[x]^* = R^*$. Assume $\deg(f) \leq \deg(g)$. Then either

$\deg(f) = 0$ and $f \mid c(h) \implies c(h) \nsim 1$, or $\deg(f) > 0 \implies h$ reducible in $F[x]$.

($\implies$): If h is irreducible in $R[x]$, then obviously h is primitive. Let $h = fg$ in $F[x]$, with f, g both of positive degree. By III.K.2, $f = \alpha f_0$, $g = \beta g_0$ (with $f_0, g_0 \in R[x]$ primitive, and $\alpha, \beta \in F^*$) $\implies$ $h = \alpha\beta f_0 g_0$. By III.K.6, $f_0 g_0$ is primitive. By (III.K.5), $f_0 g_0 \sim h \implies \alpha\beta \in R^* \implies h = (\alpha\beta f_0)g_0$ is reducible in $R[x]$, a contradiction. $\square$

Recall that we are assuming R is a UFD.

III.K.8. THEOREM. *$R[x]$ is a UFD.* (*In particular, $\mathbb{Z}[x]$ is one.*)

So uniqueness of factorization is stable under adjoining indeterminates, unlike the property of having all ideals be principal.

III.K.9. COROLLARY. *$R[x_1, \ldots, x_n]$ is a UFD.* (*So for $\mathbb{F}$ any field, $\mathbb{F}[x_1, \ldots, x_n]$ is one.*)

In particular, $F[x_1, \ldots, x_n]$ is a UFD, which is fortunate since otherwise algebraic geometry would have no chance of working!

PROOF OF III.K.9. Recall that $F[x]$ is a UFD. Given $f \in R[x]\backslash\{0\}$, we have

$$\begin{aligned}
f &= c(f)g && (g \in R[x] \text{ primitive})\\
&= c(f)g_1 \cdots g_k && (g_j \in F[x] \text{ irreducibles})\\
&= c(f)(\beta_1 f_1)\cdots(\beta_k f_k) && (\beta_j \in F^*,\ f_j \in R[x] \text{ primitive})\\
&= c(f)\beta f_1 \cdots f_k && \begin{pmatrix} f_1 \cdots f_k \text{ primitive by III.K.6,} \\ \text{hence } \beta \in R^* \text{ by (III.K.5)}\end{pmatrix}\\
&= \alpha_1 \cdots \alpha_\ell f_1 \cdots f_k && (\alpha_i \in R \text{ irreducible})
\end{aligned}$$

where the last step is possible because R is a UFD. Clearly the α_i are irreducible in $R[x]$, and by III.K.7, so are the f_j.

Now we must show the essential uniqueness of this factorization. If $f = \alpha'_1 \cdots \alpha'_{\ell'} f'_1 \cdots f'_{k'}$ ($\deg(\alpha'_i) = 0$, $\deg(f'_j) > 0$) is another factorization into irreducibles in $R[x]$, then III.K.7 $\implies$ the f'_j are irreducible in $F[x]$ and primitive, whence (by III.K.6) $f'_1 \cdots f'_{k'}$

is primitive. So we get $\alpha_1 \cdots \alpha_\ell \sim \alpha'_1 \cdots \alpha'_{\ell'}$ and $f'_1 \cdots f'_{k'} \sim f_1 \cdots f_k$ by III.K.2. Since R is a UFD, $\ell = \ell'$ and $\alpha'_i \sim \alpha_{\sigma(i)}$ (in R, hence in $R[x]$) for some $\sigma \in \mathfrak{S}_\ell$. And because $F[x]$ is a UFD, $k = k'$ and $f'_j \sim f_{\pi(j)}$ (in $F[x]$, hence in $R[x]$ by III.K.2) for some $\pi \in \mathfrak{S}_k$. $\square$

III.K.10. COROLLARY. *Let $f \in R[x]$ be primitive, $g \in R[x] \backslash \{0\}$, and $f \mid g$ in $F[x]$. Then $f \mid g$ in $R[x]$.*

PROOF. Using III.K.9, write $g = \alpha_1 \cdots \alpha_j g_1 \cdots g_k$, with $\alpha_i \in R$ irreducible and $g_j \in R[x]$ irreducible of positive degree. By III.K.7, the g_j are primitive, and irreducible in $F[x]$. Hence we may write $g = (\alpha_1 \cdots \alpha_j g_1) g_2 \cdots g_k$ as a product of irreducibles in $F[x]$.

Since $f \mid g$ in $F[x]$ (and $F[x]$ is a UFD), we have $f = \beta g_{i_1} \cdots g_{i_r}$ for some $\beta \in F^*$ and $\{i_1, \ldots, i_r\} \subseteq \{1, \ldots, k\}$; note that $g_{i_1} \cdots g_{i_r}$ is primitive by III.K.6. Since f is also primtive, applying III.K.5 gives $\beta \in R^*$. So $f \mid g$ in $R[x]$. $\square$

III.K.11. COROLLARY. *Given $g \in R[x]$ monic, $f \in F[x]$ monic dividing g (in $F[x]$). Then $f \in R[x]$.*

PROOF. Write (by III.K.2) $f = \alpha h$, with $h \in R[x]$ primitive and $\alpha \in F^*$. Then $h|g$ in $F[x]$, and so (by III.K.10) $h|g$ in $R[x]$. Accordingly, we write $g = hG$, with $G \in R[x]$. Since the highest coefficient of g is 1, the highest coefficients of h and G must be units, say $u_h, u_G \in R^*$. But then f monic $\implies \alpha = u_h^{-1}$, and so $f \in R[x]$. $\square$

The main application of these results for now is to proving irreducibility for polynomials over $\mathbb{Q}$.

III.K.12. COROLLARY. *If $f \in \mathbb{Z}[x]$ is monic, then all rational roots are integers.*

PROOF. If $q \in \mathbb{Q}$ is a root, then (by III.G.16) $x - q$ divides f in $\mathbb{Q}[x]$. By III.K.11, $x - q$ must belong to $\mathbb{Z}[x]$, i.e. $q \in \mathbb{Z}$. $\square$

III.K.13. EXAMPLE. We claim that $f = x^3 - 3x - 1$ is irreducible in $\mathbb{Q}[x]$. By III.K.7, it suffices to show irreducibility in $\mathbb{Z}[x]$. If it factored there, it would have a linear factor, necessarily $x + 1$ or $x - 1$ (why?). But $f(1) = -3$ and $f(-1) = 1$ are both nonzero.

III.K.14. EISENSTEIN'S IRREDUCIBILITY CRITERION. *If* $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$, *and there exists a prime* p *such that* $p | a_i$ *(for* $i = 0, \ldots, n-1$*),* $p \nmid a_n$ *and* $p^2 \nmid a_0$*, then* f *is irreducible in* $\mathbb{Q}[x]$.

PROOF. First notice that if f is not primitive, then $p \nmid c(f)$, and $\tilde{f} := \frac{f}{c(f)}$ is primitive and still satisfies the hypotheses. Moreover, if $\tilde{f}$ is irreducible in $\mathbb{Q}[x]$, so is f. So we may assume for the rest of the proof that f is primitive.

By III.K.7, it suffices to show that f is irreducible in $\mathbb{Z}[x]$. Suppose that $f = gh$ where $g = b_0 + \cdots + b_r x^r$ and $h = c_0 + \cdots + c_s x^s$. Since f is primitive, r and s are both positive, and the assumptions yield:

- $p \mid b_0 c_0$ but $p^2 \nmid b_0 c_0$ hence (swapping g and h if needed) $p \nmid c_0$ and $p \mid b_0$; and
- $p \nmid b_r c_s$ hence $p \nmid b_r$.

Let i_0 denote the least integer i for which $p \nmid b_i$. Since $0 < i_0 \leq r < n$ we have

$$p \,\big|\, a_{i_0} = \underbrace{c_0 b_{i_0}}_{p\nmid} + \underbrace{c_1 b_{i_0 - 1} + \cdots + c_{i_0} b_0}_{p|}$$

which is a contradiction. □

III.K.15. EXAMPLE. To see that $f = x^n - p$ is irreducible in $\mathbb{Q}[x]$, simply note that the hypotheses of III.K.14 hold: p does not divide the coefficient of x^n, but divides all other coefficients, with p^2 not dividing the constant term.

The last two examples show that if $\theta \in \mathbb{R}$ satisfies $\theta^3 - 3\theta - 1$ [resp. $\theta^n = p$] then

$$\mathbb{Q}[\theta] \cong \mathbb{Q}[x]/(x^3 - 3x - 1) \quad [\text{resp.} \cong \mathbb{Q}[x]/(x^n - p)]$$

is a field, using the fact that $\mathbb{Q}[x]$ is a PID (cf. III.H.8). Since $\mathbb{Z}[x]$ is a UFD, the corresponding quotients of $\mathbb{Z}[x]$ are domains by III.I.13.