MA2215 2010–2011
A (non-examinable) proof of Gauss' lemma

We want to prove:

Gauss' lemma. If R is a UFD, then $R[x]$ is a UFD.

We know that if F is a field, then $F[x]$ is a UFD (by Proposition 47, Theorem 48 and Corollary 46). In outline, our proof of Gauss' lemma will say that if F is a field of fractions of R, then any polynomial $f \in R[x]$ is in the UFD $F[x]$, and so can be written as a product of irreducible factors in an essentially unique manner. The reason this simple argument doesn't work is that it produces factors of f in $\mathrm{Irred}(F[x])$, but not necessarily in $\mathrm{Irred}(R[x])$, and we only get uniqueness up to associates in $F[x]$, which is weaker than uniqueness up to associates in $R[x]$. It turns out that the way to get around this difficulty is to consider primitive polynomials.

Throughout, let R be a UFD.

Definition. We say that a polynomial $f \in R[x]$ is *primitive* if

$$d \in R^\times,\ d|f \implies d \in \mathrm{Units}(R).$$

This means that the only common divisors of the coefficients of f are the units of R.

For example, $15x^3 - 6x + 8$ is a primitive polynomial in $\mathbb{Z}[x]$ since the only common divisors of $15, 0, -6, 8$ are ± 1.

On the other hand, $f = 24x^3 - 18$ is a polynomial in $\mathbb{Z}[x]$ which is not primitive since $6 \in \mathbb{Z}^\times$ and $6|f$, but 6 is not a unit in $\mathbb{Z}$. In fact, we have $f = a\widetilde{f}$ where $a = 6$ and $\widetilde{f} = 4x^3 - 3$ which is primitive; and apart from sign changes (that is, up to associates in $\mathbb{Z}$) this is the only way to factor out a primitive polynomial from f. This is typical:

Lemma A.1. (a) If $f \in R[x]$ with $f \neq 0$, then $f = a\widetilde{f}$ for some $a \in R^\times$ and some primitive polynomial $\widetilde{f} \in R[x]$.

(b) If $\widetilde{f}$ and $\widetilde{g}$ are primitive polynomials in $R[x]$ and $a, b \in R^\times$ with $a\widetilde{f} = b\widetilde{g}$, then $a \| b$ in R.

Proof. (a) Suppose that $f = a_0 + \cdots + a_n x^n$ and let a be a gcd of $a_0, a_1, \ldots, a_n$ in R (this exists, since R is a UFD). Since $f \neq 0$ we have $a \neq 0$, and $a|f$ so $f = a\widetilde{f}$ for some $\widetilde{f} \in R[x]$. If $d \in R^\times$ and $d|\widetilde{f}$ then $ad|f$ so $ad|a_j$ for each j. Since a is a gcd of the a_j's, we have $ad|a$, so $d|1$ and so $d \in \mathrm{Units}(R)$. So $\widetilde{f}$ is primitive.

(b) Let d be a gcd of a and b, and let $a_0 = a/d$ and $b_0 = b/d$. Then a_0 and b_0 have gcd 1, and $a_0|a_0\widetilde{f}$ and $a_0\widetilde{f} = b_0\widetilde{g}$, so $a_0|b_0\widetilde{g}$. Since a_0 and b_0 have gcd 1, it follows that $a_0|\widetilde{g}$. Since $\widetilde{g}$ is primitive, $a_0 \in \mathrm{Units}(R)$. Similarly, $b_0 \in \mathrm{Units}(R)$. So $a_0 b_0^{-1} \in \mathrm{Units}(R)$, and $a = a_0 b_0^{-1} b$. So $a \| b$ in R. □

This factorisation $f = a\widetilde{f}$ is at the heart of what follows. The idea is to deal with the factorisation of a, which is in the UFD R, and the factorisation of the primitive polynomial $\widetilde{f}$, separately. For the second part, we first need to establish some properties of primitive polynomials.

Proposition A.2. If $f, g \in R[x]$ are both primitive, then fg is primitive.

Proof. Suppose that $f, g \in R[x]$ are both primitive, but fg is not primitive. Then there is $d \in R^\times$ with $d|fg$ so that d is not a unit. Since $d \in R$, which is a UFD, there is $p \in \text{Irred}(R)$ so that $p|d$. So $p|fg$ but since f and g are primitive and p is not a unit, we must have $p \nmid f$ and $p \nmid g$.

Let us write $f = a_0 + a_1x + \cdots + a_nx^n$, $g = b_0 + b_1x + \cdots + b_mx^m$ and $fg = c_0 + c_1x + \cdots + c_{n+m}x^{n+m}$. Then $p|fg$, so $p|c_k$ for every k. On the other hand, $p \nmid f$ so $p \nmid a_i$ for some i, and $p \nmid g$ so $p \nmid b_j$ for some j.

Let $r = \min\{i \colon 0 \le i \le n,\ p \nmid a_i\}$ and $s = \min\{j \colon 0 \le j \le m,\ p \nmid b_j\}$. Consider

$$c_{r+s} = \underbrace{a_0b_{r+s} + a_1b_{r+s-1} + \cdots + a_{r-1}b_{s+1}}_{\text{call this } \alpha} + a_rb_s + \underbrace{a_{r+1}b_{s-1} + \cdots + a_{r+s}b_0}_{\text{call this } \beta}.$$

Since $p|a_i$ for $i < r$ we have $p|\alpha$, and since $p|b_j$ for $j < s$ we have $p|\beta$, and we know that $p|c_{r+s}$. So $p|a_rb_s = c_{r+s} - \alpha - \beta$, so $p|a_r$ or $p|b_s$ by Proposition 43(a). But $p \nmid a_r$ and $p \nmid b_s$ by the definition of r and s, so this is a contradiction. □

Lemma A.3. Let R be a UFD with field of fractions F, and let $g \in F[x]$ with $g \neq 0$. There is $u \in F^\times$ so that $\widetilde{g} = ug$ is a primitive polynomial in $R[x]$.

Proof. Since F is a field of fractions of R, the coefficients of g are all of the form $a_ib_i^{-1}$ where $a_i \in R$ and $b_i \in R^\times$ for $0 \le i \le n$, where $n = \deg(g)$. Let $b = b_0b_1 \dots b_n$ be the product of the b_i's; then $b \in R^\times$ and $bg \in R[x]$. By Lemma A.1, there is $a \in R^\times$ so that $bg = a\widetilde{g}$ for some primitive $\widetilde{g} \in R[x]$, and taking $u = ba^{-1} \in F^\times$ gives $\widetilde{g} = ug$. □

The next result shows that for primitive polynomials, we get the same answers to the questions "are these associates" or "is this irreducible" whether work in $R[x]$ or in $F[x]$.

Proposition A.4. Let R be a UFD with field of fractions F.

(a) If $f, g \in R[x]$ and f and g are primitive with $f \| g$ in $F[x]$, then $f \| g$ in $R[x]$.

(b) If $f \in R[x]$ and f is primitive, then $f \in \text{Irred}(R[x]) \iff f \in \text{Irred}(F[x])$.

Proof. (a) If $f \| g$ in $F[x]$ then there is $\alpha \in \text{Units}(F[x]) = F^\times$ so that $g = \alpha f$. Since F is a field of fractions of R, we have $\alpha = ab^{-1}$ for some $a, b \in R^\times$. Hence $af = bg$. By Lemma A.1(b), $a \| b$ in R, so $\alpha = ab^{-1} \in \text{Units}(R)$. Since $g = \alpha f$ and $\alpha \in \text{Units}(R) = \text{Units}(R[x])$, we have $f \| g$ in $R[x]$.

(b) Suppose $f \in R[x]$ and f is primitive. We'll prove the equivalent statement: $f \notin \text{Irred}(R[x]) \iff f \notin \text{Irred}(F[x])$.

If $f \notin \text{Irred}(R[x])$ then $f = gh$ for some $g, h \in R[x]$ which are not in $\text{Units}(R[x])$. Since f is primitive, $f \neq 0$. So $g \neq 0$. If $g \in \text{Units}(F[x]) = F^\times$ then $g \in R^\times$. Since $g|f$ and f is primitive, we have $g \in \text{Units}(R) = \text{Units}(R[x])$, which is a contradiction. So g is not a unit in $F[x]$, and neither is h for the same reasons, and $f = gh$. So $f \notin \text{Irred}(F[x])$.

Conversely, if $f \notin \text{Irred}(F[x])$ then $f = gh$ for some $g, h \in F[x]$ which are not in $\text{Units}(F[x])$. Since $f \neq 0$ we have $g, h \neq 0$, so by Lemma A.3, there are $u, v \in F^\times$ so that $\widetilde{g} = ug$ and $\widetilde{h} = vh$ are both primitive polynomials in $R[x]$. By Proposition A.2, $\widetilde{g}\widetilde{h}$ is also a primitive polynomial in $R[x]$. Now $\widetilde{g}\widetilde{h} = (ug) \cdot (vh) = uvf$, so $\widetilde{g}\widetilde{h} \| f$ in $F[x]$, so by (a), $\widetilde{g}\widetilde{h} \| f$ in $R[x]$. Since $\widetilde{g}$ and $\widetilde{h}$ are primitive, they are not units in R, so they are not units in $R[x]$. So $\widetilde{g}\widetilde{h} \notin \text{Irred}(R[x])$, so $f \notin \text{Irred}(R[x])$. □

Proof of Gauss' lemma. Let $f \in R[x]$ be non-zero with $f \notin \text{Units}(R[x])$. We first show that f is a product of elements of $\text{Irred}(R[x])$. By Lemma A.1(a), there is $a \in R^\times$ so that $f = a\widetilde{f}$ where $\widetilde{f} \in R[x]$ is primitive. Since R is a UFD, we can factorise a as a product of elements of $\text{Irred}(R)$, and $\text{Irred}(R) \subseteq \text{Irred}(R[x])$. So it only remains to factorise the primitive polynomial $\widetilde{f}$.

Since $F[x]$ is a UFD, we have $\widetilde{f} = p_1 p_2 \dots p_n$ for some $p_i \in \text{Irred}(F[x])$. By Lemma A.3, each p_i is an associate in $F[x]$ of a primitive polynomial $\widetilde{p_i} \in R[x]$. So $\widetilde{f} \| \widetilde{p_1}\widetilde{p_2} \dots \widetilde{p_n}$ in $F[x]$. But $\widetilde{p_1}\widetilde{p_2} \dots \widetilde{p_n}$ is primitive by Proposition A.2, so by Proposition A.4(a), $\widetilde{f} \| \widetilde{p_1}\widetilde{p_2} \dots \widetilde{p_n}$ in $R[x]$, and multiplying $\widetilde{p_1}$ by a unit in R if necessary (to get another primitive polynomial in $R[x]$ which is an associate of p_1 in $F[x]$), we have $f = \widetilde{p_1}\widetilde{p_2} \dots \widetilde{p_n}$.

In fact, each $\widetilde{p_i}$ is in $\text{Irred}(R[x])$. Here's why: each p_i is in $\text{Irred}(F[x])$ and $p_i \| \widetilde{p_i}$ in $F[x]$, so $\widetilde{p_i} \in \text{Irred}(F[x])$. So by Proposition A.4(b), $\widetilde{p_i} \in \text{Irred}(R[x])$. So we have factorised $\widetilde{f}$, and hence f, as a product of polynomials in $\text{Irred}(R[x])$.

Now we have to establish uniqueness of such factorisations. We must show that if $p_1 p_2 \dots p_n = q_1 q_2 \dots q_m$ where $p_i, q_j \in \text{Irred}(R[x])$, then $n = m$ and, up to reordering, we have $p_i \| q_i$ in $R[x]$ for $1 \le i \le n$.

Observe that any non-constant irreducible polynomial in $R[x]$ must be primitive. Reorder $p_1 \dots p_n$ and $q_1 \dots q_m$ so that the constant factors appear before the non-constant (and hence primitive) factors. Then there are integers k, ℓ so that $p_i \in \text{Irred}(R)$ for $i \le k$ and p_i is primitive for $i > k$, and $q_j \in \text{Irred}(R)$ for $j \le \ell$ and q_j is primitive for $j > \ell$. Let $a = p_1 \dots p_k \in R^\times$, let $g = p_{k+1} \dots p_n$, and let $b = q_1 \dots q_\ell \in R^\times$ and $h = q_{\ell+1} \dots q_m$. Then $ag = bh$ and g and h are both primitive, by Proposition A.2. So $a \| b$ in R, by Lemma A.1(b). By unique factorisation in R, this gives $k = \ell$ and, up to reordering, $p_i \| q_i$ in R (and so also in $R[x]$) for $1 \le i \le k$.

It remains to deal with the non-constant factors. By the previous paragraph, we have $p_{k+1} \dots p_n \| q_{k+1} \dots q_m$ in $R[x]$. But for $i, j > k$, each p_i and q_j is primitive and irreducible in $R[x]$, and so is also irreducible in $F[x]$ by Proposition A.4(b). Since $F[x]$ is a UFD, we have $n = m$ and up to reordering, $p_i \| q_i$ in $F[x]$ for $k < i \le n$. By Proposition A.4(a), $p_i \| q_i$ in $R[x]$ for $k < i \le n$.

The previous two paragraphs show that $n = m$ and up to reordering, $p_i \| q_i$ in $R[x]$ for $1 \le i \le n$, as required. So $R[x]$ is a UFD. □

Remark. The name "Gauss' lemma" may also refer to some of the results we used along the way. For example, it may refer to Proposition A.2, or to Proposition A.4(b), sometimes in the special case that $R = \mathbb{Z}$ and $F = \mathbb{Q}$. This latter result states that a primitive polynomial is irreducible over $\mathbb{Q}$ if and only if it is irreducible over $\mathbb{Z}$.

By way of an example, let's use this result to quickly show that $f = x^3 - 3x - 1$ is in $\text{Irred}(\mathbb{Q}[x])$. First we'll show that $f \in \text{Irred}(\mathbb{Z}[x])$. If $a, b \in \mathbb{Z}$ with $ax - b | f$ in $\mathbb{Z}[x]$ then by examining the coefficient of x^3 and the constant term, we see that $a|1$ and $b|-1$ in $\mathbb{Z}$, so $a, b \in \{1, -1\}$, so $x-1|f$ or $x+1|f$. But $f(1) \neq 0$ and $f(-1) \neq 0$, so this is impossible. So f has no degree 1 factors in $\mathbb{Z}[x]$. Moreover, f is primitive, so f has no degree 0 factors in $\mathbb{Z}[x]$ apart from units. Since f has degree 3, this shows that $f \in \text{Irred}(\mathbb{Z}[x])$. Now $\mathbb{Q}$ is a field of fractions of $\mathbb{Z}$ and f is primitive, so $f \in \text{Irred}(\mathbb{Q}[x])$ by Proposition A.4(b).