Gauss' Lemma without Primes

Bruno Haible
Mathematisches Institut II
Universität Karlsruhe
Kaiserstraße 12
D – 76131 Karlsruhe
Email: <haible@ma2s2.mathematik.uni-karlsruhe.de>

Started: 3 November 1990
Last change: 19 April 1994

Mathematics Subject Classification: 13A05.

Abstract: We prove a form of Gauss' lemma which holds in a wider class of rings than the factorial rings.

1. GCD Rings

DEFINITION 1:
A *GCD ring* is an integral domain R such that every two elements $a, b \in R$ have a $\gcd(a, b)$ (that is, a $d \in R$ such that $d \mid a$, $d \mid b$, $(c \mid a \wedge c \mid b \Rightarrow c \mid d)$).

Note: Factorial rings are GCD rings. (For if R is factorial and $a, b \in R \setminus \{0\}$ then $\prod\limits_p p^{\min(\mathrm{ord}_p(a), \mathrm{ord}_p(b))}$ is a $\gcd(a, b)$.)

Note (W. TRINKS): Not every GCD ring is factorial. (Put $R = \bigcup\limits_{n=1}^{\infty} k\big[X^{1/n}\big]$ where k is a field.)

In an integral domain, two elements a, b are called *associated* (or *multiplicatively equivalent*: $a \approx b$) if $a \mid b$ and $b \mid a$. This is an equivalence relation, and $a \approx b \Leftrightarrow b \in a \cdot R^\times$. See [Ja], section 2.14.

From now on, let R be a GCD ring.

LEMMA 1:
Let $a, b, c, \ldots$ in R.

(a) $\gcd(a, b)$ is unique up to associates.
(b) $\gcd(a, b) = 0$ iff $a = 0$ and $b = 0$.
(c) If $a' \mid a$ and $b' \mid b$ then $\gcd(a', b') \mid \gcd(a, b)$.
(d) $\gcd(a, b + ac) \approx \gcd(a, b)$.
(e) $\gcd(ac, bc) \approx \gcd(a, b) \cdot c$.
(f) $\gcd(a, bc) \mid \gcd(a, b) \cdot \gcd(a, c)$.
(g) $\gcd(a, \gcd(b, c)) \approx \gcd(\gcd(a, b), c)$.
(h) gcd is a commutative and associative binary operation on $R/R^\times$. To any $a_1, \ldots, a_n \in R$ $(n \in \mathbb{N} \setminus \{0\})$ a $\gcd(a_1, \ldots, a_n)$ can be defined; it is invariant under permutation of the a_i and is uniquely defined up to associates by the condition

$$(\forall i : d \mid a_i) \wedge ((\forall i : c \mid a_i) \Rightarrow c \mid d).$$

(i) If $a_1, \ldots, a_n \in R$ $(n \in \mathbb{N} \setminus \{0\})$, then there is a $d \in R$ such that $a_1 = d \cdot a_1{}', \ldots, a_n = d \cdot a_n{}'$ and $\gcd(a_1{}', \ldots, a_n{}') \approx 1$.
(j) $\gcd(a, b_1 + ac_1, \ldots, b_n + ac_n) \approx \gcd(a, b_1, \ldots, b_n)$.

Proof:
(See also [Ja], section 2.14.)

(a) If d and d' are two gcds of a and b, then $d \mid d'$ and $d' \mid d$.
(b) Immediate.
(c) Let $d = \gcd(a', b')$. Then $d \mid a' \mid a$ and $d \mid b' \mid b$.
(d) If $d \mid a$, then $d \mid b + ac$ is equivalent to $d \mid b$.
(e) By (b), we may assume $c \neq 0$. Put $d = \gcd(a, b)$ and $e = \gcd(ac, bc)$. One easily sees $d \cdot c \mid e$. From $\frac{e}{c} \mid a$ and $\frac{e}{c} \mid b$ one gets $\frac{e}{c} \mid d$, so $e \mid d \cdot c$.
(f) Obviously $\gcd(a, bc) \mid a \mid a \cdot \gcd(a, c)$. By (c) and (e), one has $\gcd(a, bc) \mid \gcd(ab, bc) \approx b \cdot \gcd(a, c)$. Combine this using (e): $\gcd(a, bc) \mid \gcd(a \cdot \gcd(a, c), b \cdot \gcd(a, c)) \approx \gcd(a, b) \cdot \gcd(a, c)$.
(g) Obvious.
(h) Obvious.
(i) Put $d = \gcd(a_1, \ldots, a_n)$. If $d = 0$, let all $a_i{}' = 1$. Else put $a_i{}' = \frac{a_i}{d}$, and from (e) we get $d \approx d \cdot \gcd(a_1{}', \ldots, a_n{}')$.
(j) By (d), we have

$$\begin{aligned}\gcd(a, b_1 + ac_1, \ldots, b_n + ac_n) &\approx \gcd(a, \gcd(a, b_1 + ac_1), \ldots, \gcd(a, b_n + ac_n)) \\ &\approx \gcd(a, \gcd(a, b_1), \ldots, \gcd(a, b_n)) \\ &\approx \gcd(a, b_1, \ldots, b_n).\end{aligned}$$

q.e.d.

PROPOSITION 2:
Every two elements $a, b \in R$ have a $\operatorname{lcm}(a, b)$ (that is, an $e \in R$ such that $a \mid e$, $b \mid e$, $(a \mid f \wedge b \mid f \Rightarrow e \mid f)$). The $\operatorname{lcm}(a, b)$ is uniquely defined up to associates. We have $\gcd(a, b) \cdot \operatorname{lcm}(a, b) \approx a \cdot b$.

Proof:
Let's first prove the existence of $\operatorname{lcm}(a, b)$. Put $d = \gcd(a, b)$. If $d = 0$, we put $e = 0$ and are done. If $d \neq 0$, put $e := \frac{ab}{d} \in R$. We have $a \mid a \cdot \frac{b}{d} = e$ and $b \mid \frac{a}{d} \cdot b = e$. For any $f \in R$ with $a \mid f$ and $b \mid f$, put $f' = \gcd(ab, f)$. We then also have $a \mid f'$ and $b \mid f'$. If $f' \neq 0$ then consider $\frac{ab}{f'}$ which divides a and b. It follows that $e \mid f' \mid f$. So e is a $\operatorname{lcm}(a, b)$.
Uniqueness: If e and e' are two lcms, then $e \mid e'$ and $e' \mid e$. **q.e.d.**

LEMMA 3:
Let $a, b, c, \ldots$ in R.

(a) $\operatorname{lcm}(a, b) = 0$ iff $a = 0$ or $b = 0$.
(b) If $a' \mid a$ and $b' \mid b$ then $\operatorname{lcm}(a', b') \mid \operatorname{lcm}(a, b)$.
(c) $\operatorname{lcm}(ac, bc) \approx \operatorname{lcm}(a, b) \cdot c$.
(d) $\operatorname{lcm}(a_1 a_2, b_1 b_2) \mid \operatorname{lcm}(a_1, b_1) \cdot \operatorname{lcm}(a_2, b_2)$.
(e) $\operatorname{lcm}(a, bc) \mid \operatorname{lcm}(a, b) \cdot \operatorname{lcm}(a, c)$.
(f) $\operatorname{lcm}(a, \operatorname{lcm}(b, c)) \approx \operatorname{lcm}(\operatorname{lcm}(a, b), c)$.
(g) lcm is a commutative and associative binary operation on $R/_{R^\times}$. To any $a_1, \ldots, a_n \in R$ $(n \in \mathbb{N} \setminus \{0\})$ a $\operatorname{lcm}(a_1, \ldots, a_n)$ can be defined; it is invariant under permutation of the a_i and is uniquely defined up to associates by the condition
$$(\forall i : d \mid a_i) \wedge ((\forall i : c \mid a_i) \Rightarrow c \mid d).$$

Proof:

(a) Immediate.
(b) Let $e = \operatorname{lcm}(a, b)$. Then $a' \mid a \mid e$ and $b' \mid b \mid e$.
(c) By (a), we may assume $c \neq 0$. Put $e = \operatorname{lcm}(a, b)$ and $f = \operatorname{lcm}(ac, bc)$. One easily sees $f \mid e \cdot c$. From $a \mid \frac{f}{c}$ and $b \mid \frac{f}{c}$ one gets $e \mid \frac{f}{c}$, so $e \cdot c \mid f$.
(d) $a_1 a_2$ and $b_1 b_2$ both divide $\operatorname{lcm}(a_1, b_1) \cdot \operatorname{lcm}(a_2, b_2)$.

(e) By (b) and (d), $\operatorname{lcm}(a, bc) \mid \operatorname{lcm}(aa, bc) \mid \operatorname{lcm}(a, b) \cdot \operatorname{lcm}(a, c)$.
(f) Obvious.
(g) Obvious.

q.e.d.

LEMMA 4:

(a) $\operatorname{lcm}(\gcd(a, b), c) \approx \gcd(\operatorname{lcm}(a, c), \operatorname{lcm}(b, c))$.
(b) $\gcd(\operatorname{lcm}(a, b), c) \approx \operatorname{lcm}(\gcd(a, c), \gcd(b, c))$.

Proof:

(a) Put $d = \gcd(a, b)$. From $d \mid a$ we get $\operatorname{lcm}(d, c) \mid \operatorname{lcm}(a, c)$, from $d \mid b$ we get $\operatorname{lcm}(d, c) \mid \operatorname{lcm}(b, c)$. Combine both to get $\operatorname{lcm}(d, c) \mid \gcd(\operatorname{lcm}(a, c), \operatorname{lcm}(b, c))$. For the other direction, write $a = d \cdot a'$, $b = d \cdot b'$ with $\gcd(a', b') \approx 1$. Then $\operatorname{lcm}(a, c) \mid \operatorname{lcm}(a, ca') \approx \operatorname{lcm}(d, c) \cdot a'$ and $\operatorname{lcm}(b, c) \mid \operatorname{lcm}(b, cb') \approx \operatorname{lcm}(d, c) \cdot b'$. So by Lemma 1(c):
$\gcd(\operatorname{lcm}(a, c), \operatorname{lcm}(b, c)) \mid \gcd(\operatorname{lcm}(d, c) \cdot a', \operatorname{lcm}(d, c) \cdot b') \approx \operatorname{lcm}(d, c) \cdot \gcd(a', b') \approx \operatorname{lcm}(d, c)$.
(b) Write $a = d \cdot a'$, $b = d \cdot b'$, $c = d \cdot c'$ with $d = \gcd(a, b, c)$ and $\gcd(a', b', c') \approx 1$. $\operatorname{lcm}(a', b') \mid \gcd(a', b') \cdot \operatorname{lcm}(a', b') \approx a'b'$ implies
$\gcd(\operatorname{lcm}(a', b'), c') \mid \gcd(a'b', c') \mid \gcd(a', c')\gcd(b', c') \approx \operatorname{lcm}(\gcd(a', c'), \gcd(b', c')) \cdot \gcd(a', b', c') \approx \operatorname{lcm}(\gcd(a', c'), \gcd(b', c'))$. Multiplying this by d, we get $\gcd(\operatorname{lcm}(a, b), c) \mid \operatorname{lcm}(\gcd(a, c), \gcd(b, c))$. On the other hand, from $a \mid \operatorname{lcm}(a, b)$ we get $\gcd(a, c) \mid \gcd(\operatorname{lcm}(a, b), c)$, from $b \mid \operatorname{lcm}(a, b)$ we get $\gcd(b, c) \mid \gcd(\operatorname{lcm}(a, b), c)$, and this gives $\operatorname{lcm}(\gcd(a, c), \gcd(b, c)) \mid \gcd(\operatorname{lcm}(a, b), c)$.

q.e.d.

COROLLARY 5:

(a) $\left({R}/{R^\times}, \gcd, \operatorname{lcm}\right)$ is a distributive lattice; the neutral elements for $\gcd$ and lcm are $0 \cdot R^\times$ and $1 \cdot R^\times$, respectively.
(b) $\left({(R \setminus \{0\})}/{R^\times}, \gcd, \operatorname{lcm}\right)$ is a distributive lattice.

Proof:
Obvious from the previous lemmas. **q.e.d.**

Note: Several other statements usually considered “typical for factorial rings” hold in GCD rings, for example:

(i) $\gcd(a + b, \operatorname{lcm}(a, b)) \approx \gcd(a, b)$.
(ii) $\gcd(a^m - 1, a^n - 1) \approx a^{\gcd(m,n)} - 1$ for $m, n \in \mathbb{N}$.
(iii) If $a^n \mid b^n$ and $n \in \mathbb{N} \setminus \{0\}$, then $a \mid b$.

2. Gauss' Lemma

Let's continue to assume that R is a GCD ring.

DEFINITION 2:
The *content* of a polynomial $f(X) = a_n X^n + \cdots + a_0 X^0 \in R[X]$ is defined as $\text{cont}\,(f) := \gcd\,(a_n, \ldots, a_0) \in {}^{R}/_{R^\times}$. If $\text{cont}\,(f) \approx 1$, f is called *primitive*.

THEOREM 6:
Gauss' Lemma: For $f, g \in R[X]$ we have $\text{cont}\,(fg) \approx \text{cont}\,(f) \cdot \text{cont}\,(g)$.

Proof:
Write $f = a_n X^n + \cdots + a_0 X^0$, $g = b_m X^m + \cdots + b_0 X^0$ and $fg = c_{n+m} X^{n+m} + \cdots + c_0 X^0$. We prove the claim by induction on $n + m$. If $m = 0$, then $\text{cont}\,(fg) = \gcd\,(a_n b_0, \ldots, a_0 b_0) \approx \gcd\,(a_n, \ldots, a_0) b_0 \approx \text{cont}\,(f) \cdot \text{cont}\,(g)$. Similarly for $n = 0$. Now let $m > 0$, $n > 0$. We may assume f and g to be primitive. (Otherwise write $f = \text{cont}\,(f) \cdot \widetilde{f}$, $g = \text{cont}\,(g) \cdot \widetilde{g}$ with $\widetilde{f}$, $\widetilde{g}$ being primitive by Lemma 1(i), observe that $\widetilde{f}\widetilde{g}$ will be primitive, and compute $\text{cont}\,(fg) = \text{cont}\left(\text{cont}\,(f)\text{cont}\,(g) \cdot \widetilde{f}\widetilde{g}\right) \approx \text{cont}\,(f)\text{cont}\,(g) \cdot \text{cont}\left(\widetilde{f}\widetilde{g}\right) \approx \text{cont}\,(f)\text{cont}\,(g)$.) By Lemma 1(f),

$$\begin{aligned}
\text{cont}\,(fg) &= \gcd\,(c_{n+m}, \ldots, c_0) \\
&\approx \gcd\,(a_n b_m, \gcd\,(c_{n+m-1}, \ldots, c_0)) \\
&\mid \gcd\,(a_n, \gcd\,(c_{n+m-1}, \ldots, c_0)) \cdot \gcd\,(b_m, \gcd\,(c_{n+m-1}, \ldots, c_0))
\end{aligned}$$

By Lemma 1(j),

$$\begin{aligned}
\gcd\,(a_n, \gcd\,(c_{n+m-1}, \ldots, c_0)) &\approx \gcd\,(a_n, c_{n+m-1}, \ldots, c_0) \\
&\approx \gcd\,(a_n, c_{n+m-1} - a_n b_{m-1}, \ldots, c_n - a_n b_0, c_{n-1}, \ldots, c_0) \\
&\approx \gcd\,(a_n, \text{cont}\,((f - a_n X^n) g))
\end{aligned}$$

The induction hypothesis gives $\text{cont}\,((f - a_n X^n) g) \approx \text{cont}\,(f - a_n X^n)\text{cont}\,(g) \approx \text{cont}\,(f - a_n X^n)$, and we get

$$\begin{aligned}
\gcd\,(a_n, \gcd\,(c_{n+m-1}, \ldots, c_0)) &\approx \gcd\,(a_n, \text{cont}\,((f - a_n X^n) g)) \approx \gcd\,(a_n, \text{cont}\,(f - a_n X^n)) \\
&\approx \text{cont}\,(f) \approx 1
\end{aligned}$$

Similarly, $\gcd\,(b_m, \gcd\,(c_{n+m-1}, \ldots, c_0)) \approx 1$. This proves $\text{cont}\,(fg) \approx 1$. **q.e.d.**

THEOREM 7:
$R[X]$ is a GCD ring.

Proof:
Let $f, g \in R[X]$. We have to find a gcd d of f and g. If $f = 0$, put $d = g$, and we are done. Similarly for $g = 0$: put $d = f$.
We now assume $f \neq 0$, $g \neq 0$. Write $f = \text{cont}\,(f) \cdot \widetilde{f}$ and $g = \text{cont}\,(g) \cdot \widetilde{g}$, with $\widetilde{f}$, $\widetilde{g}$ being primitive by Lemma 1(i). Let $K = \text{Quot}\,(R)$ the quotient field of R. The Euclidean algorithm produces $\widetilde{d} := \gcd\left(\widetilde{f}, \widetilde{g}\right)$ in $K[X]$, with $\widetilde{d} \in \widetilde{f} \cdot K[X] + \widetilde{g} \cdot K[X]$. We may assume $\widetilde{d}$ to lie in $R[X]$ (otherwise multiply $\widetilde{d}$ by the common denominator of its coefficients). We may also assume $\widetilde{d}$ to be primitive (otherwise divide $\widetilde{d}$ by its content). Now put $d := \gcd\,(\text{cont}\,(f), \text{cont}\,(g)) \cdot \widetilde{d}$.
We first claim that $\widetilde{d}$ is a gcd of $\widetilde{f}$ and $\widetilde{g}$ in $R[X]$. First, since $\widetilde{d} \mid \widetilde{f}$ in $K[X]$, we can write $\frac{\widetilde{f}}{\widetilde{d}} = \frac{a}{b} k$ with $a, b \in R \setminus \{0\}$ and a primitive $k \in R[X]$. Examining the content of $b\widetilde{f} = ak\widetilde{d}$, one sees $a \approx b$, therefore $\frac{\widetilde{f}}{\widetilde{d}} \in R[X]$. So, $\widetilde{d} \mid \widetilde{f}$ in $R[X]$, and similarly $\widetilde{d} \mid \widetilde{g}$ in $R[X]$. Second, since $\widetilde{d} \in \widetilde{f} \cdot K[X] + \widetilde{g} \cdot K[X]$, there are $u, v \in R[X]$, $c \in R \setminus \{0\}$ with $c \cdot \widetilde{d} = u \cdot \widetilde{f} + v \cdot \widetilde{g}$. If a polynomial $h \in R[X]$ divides both $\widetilde{f}$ and $\widetilde{g}$, then $h \mid c \cdot \widetilde{d}$ and $\text{cont}\,(h) \mid \text{cont}\left(\widetilde{f}\right) \approx 1$. Writing $\frac{c\widetilde{d}}{h} = \frac{a}{b} k$ with $a, b \in R \setminus \{0\}$ and a primitive $k \in R[X]$ and examining the content of $bc\widetilde{d} = ahk$, one sees $bc \approx a$, therefore $\frac{\widetilde{d}}{h} = \frac{a}{bc} k \approx k \in R[X]$, and h divides $\widetilde{d}$.

We now claim that d is a gcd of f and g in $R[X]$. It is trivial that $d = \gcd(\mathrm{cont}\,(f), \mathrm{cont}\,(g)) \cdot \widetilde{d} \mid \mathrm{cont}\,(f) \cdot \widetilde{f} = f$ and similarly $d \mid g$. Now let $h \in R[X]$ divide both f and g. Write $h = \mathrm{cont}\,(h) \cdot \widetilde{h}$ with a primitive $\widetilde{h}$. From $h \mid f$ it follows that $\mathrm{cont}\,(h) \mid \mathrm{cont}\,(f)$ and $\widetilde{h} \mid \widetilde{f}$. (To see this, write $k := \frac{f}{h} = \mathrm{cont}\,(k) \cdot \widetilde{k}$. From $f = hk$ it follows that $\mathrm{cont}\,(f) \approx \mathrm{cont}\,(h)\mathrm{cont}\,(k)$ and therefore $\widetilde{f} \approx \frac{f}{\mathrm{cont}\,(h)\mathrm{cont}\,(k)} = \widetilde{h}\widetilde{k}$.) Similarly, $\mathrm{cont}\,(h) \mid \mathrm{cont}\,(g)$ and $\widetilde{h} \mid \widetilde{g}$. We conclude $\mathrm{cont}\,(h) \mid \gcd(\mathrm{cont}\,(f), \mathrm{cont}\,(g))$, $\widetilde{h} \mid \widetilde{d}$ and therefore $h \mid d$.

q.e.d.

Corollary 8:
$R[X_1, \ldots, X_n]$ is a GCD ring.

Proof:
Repeated application of Theorem 7. **q.e.d.**

3. References

[Ja] Nathan Jacobson: Basic Algebra I.
Freeman 1985.