Math 113. Gauss’s Lemma and a Corollary (Revised)

This handout gives proofs of Gauss’s Lemma and its corollary, as presented in class on Thursday, November 7. We start with a definition.

**Definition.** A polynomial \( f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x] \) is primitive if \( f \neq 0 \) and \( \gcd(a_0, \ldots, a_n) = 1 \) (in other words, if there is no prime \( p \) such that \( p \mid a_i \) for all \( i \)).

**Theorem** (Gauss’s Lemma). Let \( g, h \in \mathbb{Z}[x] \). If both \( g \) and \( h \) are primitive, then so is their product \( gh \).

**Proof.** Write
\[
g(x) = a_n x^n + \cdots + a_0, \quad h(x) = b_m x^m + \cdots + b_0, \quad \text{and} \quad g(x)h(x) = c_n + m x^{n+m} + \cdots + c_0.
\]

Let \( p \) be a prime number. Since \( \gcd(a_0, \ldots, a_n) = 1 \) there is an integer \( j \) such that \( p \nmid a_j \). Choose the largest such \( j \). Similarly, let \( k \) be the largest integer such that \( p \nmid b_k \). Then (taking \( a_i = 0 \) for all \( i > n \) and \( b_j = 0 \) for all \( j > m \)), we have
\[
c_{j+k} = \sum_{i=0}^{m+n} a_i b_{j+k-i} = \sum_{i=0}^{j-1} a_i b_{j+k-i} + a_j b_k + \sum_{i=j+1}^{m+n} a_i b_{j+k-i}.
\]

As in an earlier proof (of the fact that if \( R \) is an integral domain then so is \( R[x] \)), the first sum is a multiple of \( p \) because \( j + k - i > k \) for all \( i < j \), and therefore \( p \mid b_{j+k-i} \) for all \( i < j \), the second sum is a multiple of \( p \) because \( p \mid a_i \) for all \( i > j \), and the term \( a_j b_k \) is not a multiple of \( p \) because neither factor is. Therefore \( p \nmid c_{j+k} \), so \( p \nmid \gcd(c_0, \ldots, c_{n+m}) \). Since this is true for all \( p \), \( \gcd(c_0, \ldots, c_{n+m}) = 1 \), and so \( gh \) is primitive.

**Lemma 1.** Let \( f \in \mathbb{Q}[x] \) be a nonzero polynomial. Then there exist unique \( c \in \mathbb{Q} \) and \( f_0 \in \mathbb{Z}[x] \) such that \( f = cf_0 \), \( c > 0 \), and \( f_0 \) is primitive. Moreover, \( f \in \mathbb{Z}[x] \) if and only if \( c \) is an integer.

**Proof.** Pick an integer \( s > 0 \) such that \( sf \in \mathbb{Z}[x] \), and write \( sf = a_n x^n + \cdots + a_0 \). Let \( r = \gcd(a_n, \ldots, a_0) \), let \( c = r/s \), and let \( f_0 = c^{-1} f \). Then it is easy to see that \( c \in \mathbb{Q} \), \( c > 0 \), and \( f = cf_0 \). Also \( f_0 \) has integer coefficients (because \( r \mid a_i \) for all \( i \)) and is primitive (if \( e > 1 \) divides \( a_i/r \) for all \( i \) then \( er \mid a_i \) for all \( i \), contradicting the definition of \( r \) as \( \gcd \) since \( er > r \)).

Next we show uniqueness. Suppose \( c_1 \in \mathbb{Q} \) and \( f_1 \in \mathbb{Z}[x] \) also satisfy the conditions of Lemma 1 in place of \( c \) and \( f_0 \), respectively. Let \( k \in \mathbb{Z}^+ \) be an integer such that \( kc, kc_1 \in \mathbb{Z} \), and let \( g = \gcd(kc, kc_1) \). Then, letting \( m_0 = kc/g \) and \( m_1 = kc_1/g \), we have
\[
m_0 f_0 = m_1 f_1,
\]
and $m_0$ and $m_1$ are relatively prime positive integers. We claim that $m_0 = m_1$. Suppose not. Then there is a prime $p$ such that one of the $m_i$ is a multiple of $p$ and the other is not. We may assume that $p | m_0$ but $p \nmid m_1$. Then $m_0 f_0$ is a polynomial in $\mathbb{Z}[x]$, all of whose coefficients are multiples of $p$, but $m_1 f_1$ is not such a polynomial. This is a contradiction; therefore $m_0 = m_1$, which gives $c_1 = c$ and $f_1 = f_0$.

Finally, suppose $f \in \mathbb{Z}[x]$. Then (in the first sentence of the proof) we may take $s = 1$, which will give $c = r \in \mathbb{Z}$. The converse is easy.

**Corollary** (Generalization of Thm. 23.11). Let $f \in \mathbb{Z}[x]$ be a nonzero polynomial. If $f$ can be factored in $\mathbb{Q}[x]$ as $f(x) = g(x)h(x)$, then it can be factored in $\mathbb{Z}[x]$ as $f(x) = \tilde{g}(x)\tilde{h}(x)$ with $\deg \tilde{g} = \deg g$ and $\deg \tilde{h} = \deg h$. (In fact, there is a $c \in \mathbb{Q}^*$ such that $\tilde{g} = c^{-1}g$ and $\tilde{h} = ch$.)

**Proof.** Pick $c \in \mathbb{Q}$ and $g_0 \in \mathbb{Z}[x]$ such that $g = cg_0$, $c > 0$, and $g_0$ is primitive. Similarly pick $d \in \mathbb{Q}$ and $h_0 \in \mathbb{Z}[x]$ such that $h = dh_0$, $d > 0$, and $h_0$ is primitive. Let $f_0 = g_0 h_0$; by Gauss's Lemma this too is primitive. Since $f = gh = cdf_0h_0 = cdf_0$ and $f \in \mathbb{Z}[x]$, we have $cd \in \mathbb{Z}$, so if we define $\tilde{g}$ and $\tilde{h}$ as in the statement of the corollary we will have $\tilde{g} = g_0 \in \mathbb{Z}[x]$ and $\tilde{h} = c h = (cd)h_0 \in \mathbb{Z}[x]$.

**Lemma 2.** Let $\phi: R \to R'$ be a ring homomorphism, and let $\psi: R[x] \to R'[x]$ be the function defined by

$$\psi(a_n x^n + \cdots + a_0) = \phi(a_n)x^n + \cdots + \phi(a_0);$$

i.e., the map from $R[x]$ to $R'[x]$ defined by applying $\phi$ to each of the coefficients. Then $\psi$ is a ring homomorphism. (Also, $\psi$ is surjective if and only if $\phi$ is.)

**Proof.** This follows from the same proof as is given in the solutions to Exercise 37a in Section 23 (on Homework 10).

(This lemma is true even if $R$ and $R'$ are not commutative. However, it will only be used here when $\phi$ is the map $\gamma_m: \mathbb{Z} \to \mathbb{Z}_m$, as in the homework exercise.)

Now we can use Lemma 2 to give a slightly different proof of Gauss's Lemma.

**Second Proof.** By contradiction. Suppose that $g,h \in \mathbb{Z}[x]$ are primitive but their product $f = gh$ is not. Let $d$ be the gcd of the coefficients of $f$; then (by assumption) $d > 1$. Let $p$ be a prime divisor of $d$, and let $\psi: \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ be the homomorphism obtained by Lemma 2 from the “reduction modulo $p$” map $\gamma_p: \mathbb{Z} \to \mathbb{Z}_p$ (this is the same map as in Exercise 37a mentioned above). Since $g$ and $h$ are primitive, $\psi(g) \neq 0$ and $\psi(h) \neq 0$. Since $\mathbb{Z}_p[x]$ is an integral domain, the product $\psi(g)\psi(h)$ is nonzero. This contradicts the fact that $\psi(gh) = 0$, which holds because all coefficients of $gh$ are in the kernel of $\gamma_p$ (i.e., are multiples of $p$).

Therefore $gh$ is primitive.