Chapter 6: Quadratic Gauss Sums

Author: Meng-Gen Tsai
Email: plover@gmail.com

Exercise 6.1. *Show that $\sqrt{2}+\sqrt{3}$ is an algebraic integer.*

Proof. Let $\alpha = \sqrt{2}+\sqrt{3}$. So $\alpha - \sqrt{2} = \sqrt{3}$. Eliminating $\sqrt{3}$ by squaring: $(\alpha-\sqrt{2})^2 = (\sqrt{3})^2$, or $\alpha^2 - 2\sqrt{2}\alpha + 2 = 3$, or $\alpha^2 - 1 = 2\sqrt{2}\alpha$. Eliminating $\sqrt{2}$ by squaring again: $(\alpha^2-1)^2 = (2\sqrt{2}\alpha)^2$, or $\alpha^4 - 2\alpha^2 + 1 = 8\alpha^2$, or $\alpha^4 - 10\alpha^2 + 1 = 0$. That is, α is a root of $x^4 - 10x^2 + 1 = 0$, i.e., α is an algebraic integer. $\square$

Actually, $x^4-10x^2+1 = (x-\sqrt{2}-\sqrt{3})(x+\sqrt{2}-\sqrt{3})(x-\sqrt{2}+\sqrt{3})(x+\sqrt{2}+\sqrt{3})$.

Proof (Proposition 6.1.5). Since $\sqrt{2}$ and $\sqrt{3}$ are algebraic integers, then $\sqrt{2}+\sqrt{3}$ is an algebraic integer by Proposition 6.1.5. (The set of algebraic integers forms a ring.) $\square$

Exercise 6.2. *Let α be an algebraic number. Show that there is an integer n such that $n\alpha$ is an algebraic integer.*

It is trivial if taking $n = 0$. So we assume that $n \neq 0$.

Proof. There exists a polynomial $f(x) = a_0x^m + a_1x^{m-1} + \cdots + a_m \in \mathbb{Q}[x]$ with $a_0 \neq 0$, such that $f(\alpha) = 0$. There exists an integer $d \neq 0$ such that $b_i = d \cdot a_i \in \mathbb{Z}$ for all $i = 1, 2, ..., m$. Therefore,

$$b_0\alpha^m + b_1\alpha^{m-1} + \cdots + b_m = 0,$$

which is not necessary a monic polynomial in $\mathbb{Z}[x]$. So we need to do a trick to absort b_0 into α, and that is why we come out multipling α by an non-zero integer $b_0 = d \cdot a_0$.

Multiply b_0^{m-1} on the both sides.

$$b_0^m\alpha^m + b_0^{m-1}b_1\alpha^{m-1} + b_0^{m-1}b_2\alpha^{m-2} + \cdots + b_0^{m-1}b_m = 0.$$
$$(b_0\alpha)^m + b_1(b_0\alpha)^{m-1} + b_0b_2(n\alpha)^{m-1} + \cdots + b_0^{m-1}b_m = 0.$$

That is, the monic polynomial $g(x) = x^m + c_1x^{m-1} + c_2x^{m-2} + \cdots + c_m \in \mathbb{Z}[x]$ (with $c_i = b_0^{i-1}b_i$ for $i = 1, 2, ..., m$) has a root $x = b_0\alpha$, i.e., $b_0\alpha$ is an algebraic integer for some integer b_0. $\square$

Exercise 6.4. *A polynomial $f(x) \in \mathbb{Z}[x]$ is said to be primitive if the greatest common divisor of its coefficients is* 1*. Prove that the product of primitive polynomials is again primitive. This is one of the many results knows as Gauss' lemma.*

Proof. Let

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n,$$
$$g(x) = b_0x^m + b_1x^{n-1} + \cdots + b_m$$

be primitive.

(1) Given prime p. Let a_i and b_j be the coefficients with the smallest index such that $p \nmid a_i$ and $p \nmid b_j$ respectively. Consider the coefficient of x^{i+j} in $f(x)g(x)$,

$$(\cdots + a_{i-1}b_{j+1}) + a_ib_j + (a_{i+1}b_{j-1} + \cdots).$$

$p \nmid a_ib_j$ since p is a prime. $p \mid (\cdots + a_{i-1}b_{j+1})$ by the definition of index i. $p \mid (a_{i+1}b_{j-1} + \cdots)$ by the definition of index j. That is, the coefficient of x^{i+j} in $f(x)g(x)$ is not divided by p.

(2) If $h(x) = f(x)g(x)$ is not primitive, there exists a prime p such that p divides all coefficients of $h(x)$. By (1), such i or j does not exist. That is, p is a factor of the greatest common divisor of $f(x)$'s or $g(x)$'s coefficients. So $f(x)$ or $g(x)$ is not primitive, which is absurd.

□

Exercise 6.16. *Let α be an algebraic number with minimal polynomial $f(x)$. Show that $f(x)$ does not have repeated roots α in $\mathbb{C}$.*

Proof. Assume not true, write $f(x) = (x-\alpha)^2g(x)$, where $g(x) \in \mathbb{C}[x]$. Differentiating $f(x)$ to get new polynomial $f'(x) \in \mathbb{Q}[x]$ and

$$\begin{aligned} f'(x) &= 2(x-\alpha)g(x) + (x-\alpha)^2g'(x) \\ &= (x-\alpha)(2g(x) + (x-\alpha)g'(x)). \end{aligned}$$

So $f'(\alpha) = 0$. Notices that $\deg f(x) \geq 2$ and thus $\deg f'(x) = \deg f(x) - 1 \geq 1$. $f'(x)$ is not zero. Thus $f(x) \mid f'(x)$ by Proposition 6.1.7, which contradicts the fact $0 < \deg f'(x) < \deg f(x)$. □

Exercise 6.17. *Show that the minimal polynomial for $\sqrt[3]{2}$ is $x^3 - 2$.*

Proof. Let $f(x) = x^3 - 2$. $f(\sqrt[3]{2}) = 0$. By Eisenstein's irreducibility criterion, $f(x)$ is irreducible over $\mathbb{Q}$. By Proposition 6.1.7, $f(x) = x^3 - 2$ is the minimal polynomial of $\sqrt[3]{2}$. □

Exercise 6.18. *Show that there exist algebraic numbers of arbitrarily high degree.*

A generalization to Exercise 6.17.

If p is a prime, then $x^n - p$ is irreducible over $\mathbb{Q}$, by Eisenstein's irreducibility criterion, so $[\mathbb{Q}(\sqrt[n]{p}) : \mathbb{Q}] = n$. (Example 1.16 in Patrick Morandi, Field and Galois Theory.)

Proof. Let $\alpha = \sqrt[n]{p}$ for any positive integer n with $n \geq 2$ and prime p. Apply the similar argument in Exercise 6.17 to show that $f(x) = x^n - p$ is the minimal polynomial of $\sqrt[n]{p}$. □

Exercise 6.23. *If $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$, $a_i \in \mathbb{Z}$ and p is a prime such that $p \mid a_i$, $i = 1, ..., n$, $p^2 \nmid a_n$. Show that $f(x)$ is irreducible over $\mathbb{Q}$ (Eisenstein's irreducibility criterion).*

Proof.

(1) *If $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$, $a_i \in \mathbb{Z}$ and p is a prime such that $p \mid a_i$, $i = 1, ..., n$, $p^2 \nmid a_n$. Then $f(x)$ is irreducible over $\mathbb{Z}$.* Assume not true. Write $f(x) = g(x)h(x)$ as a product of two non-trivial polynomials in $\mathbb{Z}[x]$,

$$g(x) = b_0 x^s + b_1 x^{s-1} + \cdots + b_s,$$
$$h(x) = c_0 x^t + c_1 x^{t-1} + \cdots + c_t,$$

where $b_0 = c_0 = 1$, $0 < s < n$, and $0 < t < n$.

Since $p \nmid b_0$, there exists largest index i such that $p \nmid b_i$. (Therefore $p \mid b_{i+1}$, $p \mid b_{i+2}$, and so on.) Similarly, there exists largest index j such that $p \nmid c_j$. ($p \mid c_{j+1}$, $p \mid c_{j+2}$, and so on.) Now we consider the coefficient a_{i+j}.

$$a_{i+j} = (\cdots + b_{i-1}c_{j+1}) + b_i c_j + (b_{i+1}c_{j-1} + \cdots).$$

$p \nmid b_i c_j$ since p is a prime. $p \mid (b_{i+1}c_{j-1} + \cdots)$ by the definition of index i. $p \mid (\cdots + b_{i-1}c_{j+1})$ By the definition of index j. Thus, $p \nmid a_{i+j}$. Hence $i = 0$ and $j = 0$. Especially, $p \mid b_s$ and $p \mid c_t$. $p^2 \mid b_s c_t$, or $p^2 \mid a_n$ which contradicts. □

(2) *$f(x)$ is irreducible over $\mathbb{Q}$ if $f(x)$ is primitive and irreducible over $\mathbb{Z}$.* Assume $f(x) = g(x)h(x) \in \mathbb{Q}[x]$ is reducible. Let a and b be the least common multiple of the denominators of $g(x)$ and $h(x)$ respectively. Then

$$ab \cdot f(x) = (a \cdot g(x))(b \cdot h(x)) = c g_0(x) d h_0(x),$$

where $g_0(x)$, $h_0(x)$ are primitive polynomials in $\mathbb{Z}[x]$, and c and d are the greatest common divisor of $(a \cdot g(x))$'s and $(b \cdot h(x))$'s coefficients respectively Since $g_0(x)h_0(x)$ is again primitive (Exercise 4),

$$ab = \pm cd, f(x) = g_0(x)h_0(x).$$

Notice that $\deg(g_0(x)) = \deg(g(x))$ and $\deg(h_0(x)) = \deg(h(x))$. So $f(x)$ is reducible over $\mathbb{Z}$, which is absurd.

□