Math 129 Problem Set 8

Lev Kruglyak

April 11, 2022

Problem 5.33.

(a) Let m be a squarefree positive integer, and assume first that $m \equiv 2$ or $3 \mod 4$. Consider the numbers $mb^2 \pm 1$, $b \in \mathbb{Z}$, and take the smallest positive b such that either $mb^2 + 1$ or $mb^2 - 1$ is a square, say a^2, $a > 0$. Then $a + b\sqrt{m}$ is a unit in $\mathbb{Z}[\sqrt{m}]$. Prove that it is the fundamental unit.

(b) Establish a similar procedure for determining the fundamental unit in $\mathcal{O}_{\mathbb{Q}[\sqrt{m}]}$ for squarefree $m > 1$, $m \equiv 1 \mod 4$.

(a) This is clear, since this procedure finds the (positive) unit with minimal b in the expression $a + b\sqrt{m}$. This is the fundamental unit since any other unit $a' + b'\sqrt{m}$ with $a', b' > 0$ must have $b' \leq b$.

(b) Recall that algebraic integers in $\mathcal{O}_{\mathbb{Q}[\sqrt{m}]}$ for $m \equiv 1 \mod 4$ are of the form $\frac{a}{2} + \frac{b}{2}\sqrt{m}$ where a and b are both odd. So if we want such an integer to have norm ± 1, this means that $a^2 + mb^2 = \pm 4$. Thus we can do the same thing we did for $2, 3 \mod 4$ except we check $mb^2 \pm 4$ for squareness, choosing odd b.

Problem 5.34. Determine the fundamental unit in $\mathcal{O}_{\mathbb{Q}[\sqrt{m}]}$ for all squarefree m, $2 \leq m \leq 30$, except for $m = 19$ and 22.

Using a simple Python program which implements the procedure from Problem 5.33, we can get the following table:

m	u	m	u
2	$1 + \sqrt{2}$	15	$4 + \sqrt{15}$
3	$2 + \sqrt{3}$	17	$4 + \sqrt{17}$
5	$\frac{1+\sqrt{5}}{2}$	19	$170 + 39\sqrt{19}$
6	$5 + 2\sqrt{6}$	21	$\frac{5+\sqrt{21}}{2}$
7	$8 + 3\sqrt{7}$	22	$\frac{197+42\sqrt{22}}{2}$
10	$3 + \sqrt{10}$	23	$24 + 5\sqrt{23}$
11	$10 + 3\sqrt{11}$	26	$5 + \sqrt{26}$
13	$\frac{3+\sqrt{13}}{2}$	29	$\frac{5+\sqrt{29}}{2}$
14	$15 + 4\sqrt{14}$	30	$11 + 2\sqrt{30}$

Problem 5.36. Let $\alpha = \sqrt[3]{2}$. Recall that $\mathcal{O}_{\mathbb{Q}[\alpha]} = \mathbb{Z}[\alpha]$ and $\Delta_{\mathbb{Q}[\alpha]} = -108$.

(a) Show that $u^3 > 20$, where u is the fundamental unit in $\mathbb{Z}[\alpha]$.

(b) Show that $\beta = (\alpha - 1)^{-1}$ is a unit between 1 and u^2; conclude that $\beta = u$.

(a) By Problem 5.35, we know that if $|\Delta_{\mathbb{Q}[\alpha]}| \geq 33$, then

$$u^3 > \frac{|\Delta_{\mathbb{Q}[\alpha]}| - 27}{4} = 20.25$$

which completes the proof.

(b) First, note that by Problem 2.41 we have $\mathrm{N}(\alpha - 1) = (-1)^3 + 2 = 1$, so $\alpha - 1$ and β are units. Next, since $\alpha - 1 < 1$, it follows that $\beta = \frac{1}{\alpha - 1} > 1$. We know by (a) that $u^3 > 20$ so $u^2 > \sqrt[3]{20^2} > 7$, and we know that $\beta < 7$ since if $\frac{1}{\alpha-1} > 7$ then $8 > 7\alpha$ which is impossible since cubing both sides gives $512 > 686$. So $1 < \alpha - 1 < u^2$. However since u is the fundamental unit (we know there must be a single on by Dirichlet's unit theorem), it follows that $\beta = u$. So $u = 1 + \sqrt[3]{2} + \sqrt[3]{4}$.

Problem 5.37.

(a) Show that if α is a root of a monic polynomial f over $\mathbb{Z}$, and if $f(r) = \pm 1$, $r \in \mathbb{Z}$, then $\alpha - r$ is a unit in $\mathcal{O}_{\overline{\mathbb{Q}}}$.

(b) Find the fundamental unit in $\mathcal{O}_{\mathbb{Q}[\alpha]}$ when $\alpha = \sqrt[3]{7}$.

(c) Find the fundamental unit in $\mathcal{O}_{\mathbb{Q}[\alpha]}$ when $\alpha = \sqrt[3]{3}$.

(a) Let $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$ be the monic polynomial. Note that

$$\begin{aligned} f(\alpha) - f(r) &= (\alpha^n - r^n) + c_{n-1}(\alpha^{n-1} - r^{n-1}) + \cdots + c_1(\alpha - r) = \pm 1 \\ &= (\alpha - r)\left(\frac{\alpha^n - r^n}{\alpha - r} + c_{n-1}\frac{\alpha^{n-1} - r^{n-1}}{\alpha - r} + \cdots + c_1\right) = \pm 1 \end{aligned}$$

so $(\alpha - r)$ is a unit since $\alpha^k - r^k$ is divisible by $\alpha - r$.

(b) Consider the monic polynomial $f(x) = x^3 - 7$. Note that $f(2) = 1$ so $\alpha - 2$ is a unit in $\mathcal{O}_{\mathbb{Q}[\alpha]}$. Since we want our fundamental unit to be greater than 1, consider

$$u = \frac{1}{2 - \alpha} = \frac{2^3 - \alpha^3}{2 - \alpha} = \boxed{\alpha^2 + 2\alpha + 4}.$$

This is a unit greater than one, indeed $u \approx 11.49$. To prove that this is the fundamental unit, suppose for the sake of contradiction that there was some smaller unit $u' > 1$ with $u = (u')^k$ for some $k > 1$. Then by Problem 5.35d, we would have

$$(u')^3 > \frac{|\Delta_{\mathbb{Q}[\alpha]}| - 27}{4} = 324 \implies u' > 6.87.$$

However since $u = (u')^k$, we know that $u' \leq \sqrt{u} < 4$ which is a contradiction. So u is the fundamental unit.

(c) Note that α^2 is a root of the monic polynomial $f(x) = x^3 - 9$, and $f(2) = -1$ so by (a), $\alpha^2 - 2$ is a unit. As in (b), consider

$$u = \frac{1}{\alpha^2 - 2} = \frac{\alpha^6 - 2^3}{\alpha^2 - 2} = \alpha^4 + 2\alpha^2 + 4 = \boxed{2\alpha^2 + 3\alpha + 4}.$$

Again, using the same argument as in (b), if there were a smaller unit $u' > 1$ with $u = (u')^k$ for some $k > 1$, we would have

$$(u')^3 > \frac{|\Delta_{\mathbb{Q}[\alpha]}| - 27}{4} = 54 \implies u' > 3.77.$$

Yet $u' \le \sqrt{u} < 3.54$ so we have a contradiction, and so u is the fundamental unit.

Problem 5.38.

(a) Show that $x^3 + x - 3$ has only one real root α, and $\alpha > 1.2$.

(b) Using Problem 2.28, show that $\operatorname{disc}(\alpha)$ is squarefree; conclude that it is equal to $\Delta_{\mathbb{Q}[\alpha]}$.

(c) Find the fundamental unit in $\mathcal{O}_{\mathbb{Q}[\alpha]}$.

(a) If $f(x) = x^3 + x - 3$ then $f'(x) = 3x^2 + 1$, which is always positive, meaning $f(x)$ is strictly increasing. So $f(x)$ intersects the line $y = 0$ only once, corresponding to only one real root α of $f(x)$. Note that $f(1.2) = -0.072$ so $\alpha > 1.2$. To get an every better bound, note that $f(1.3) = 0.497$ so $1.2 < \alpha < 1.3$.

(b) By Problem 2.28c, we have $\operatorname{disc}(\alpha) = -(4 \cdot 1^3 + 27 \cdot (-3)^2) = -247$, which is squarefree since $247 = 13 \cdot 19$. Then by Problem 2.40a it follows that because $\operatorname{disc}(\alpha)$ is squarefree, then $\operatorname{disc}(\alpha) = \Delta_{\mathbb{Q}[\alpha]}$.

(c) Notice that $f(1) = -1$, so by Problem 5.37a, it follows that $\alpha - 1$ is a unit. This isn't the fundamental unit since by (a), $0.2 < \alpha < 0.3$. So consider the unit

$$u = \frac{1}{\alpha - 1} = \frac{(\alpha^3 + \alpha - 3) - (1^3 + 1 - 3)}{\alpha - 1} = \frac{(\alpha^3 - 1) + (\alpha - 1)}{\alpha - 1} = \boxed{\alpha^2 + \alpha + 2}.$$

Again, using the bound from (a), we get $4.64 < u < 4.99$. If there were another unit $u' > 1$ with $u = (u')^k$, then by Problem 5.35d we would have

$$(u')^3 > \frac{|\Delta_{\mathbb{Q}[\alpha]}| - 27}{4} = 61.5 \implies u' > 3.94.$$

However this is a contradiction because $u' \le \sqrt{u}$ and $2.15 < \sqrt{u} < 2.24$. So u is the fundamental unit.

Problem 5.39. Let $\alpha^3 = 2\alpha + 3$. Verify that $\alpha < 1.9$ and find the fundamental unit in $\mathcal{O}_{\mathbb{Q}[\alpha]}$.

Notice that α is a real root of the polynomial $f(x) = x^3 - 2x - 3$. A simple argument involving derivatives shows that this has only one real root, so α is uniquely defined, and $\mathbb{Q}[\alpha]$ has only one real embedding so we can use Problem 5.35 later. This argument also gives a simple bound $1.8 < \alpha < 1.9$. Notice that $f(2) = 1$ so by Problem 5.37a we know that $\alpha - 2$ is a unit. Then we have a unit

$$u = \frac{1}{2 - \alpha} = \frac{f(2) - f(\alpha)}{2 - \alpha} = \frac{(2^3 - \alpha^3) - 2(2 - \alpha)}{2 - \alpha} = \boxed{\alpha^2 + 2\alpha + 2}.$$

We claim this is the fundamental unit, if $u' > 1$ is another unit with $u = (u')^k$, then by Problem 5.35d and Problem 2.28 we have

$$(u')^3 > \frac{|\Delta_{\mathbb{Q}[\alpha]}| - 27}{4} = \frac{|-(4 \cdot (-2)^3 + 27 \cdot (-3)^3)| - 27}{4} = 46 \implies u' > 3.58.$$

On the other hand, we have $u' < \sqrt{u}$ yet $\sqrt{u} < 3.07$, a contradiction. So u is the fundamental unit.