Math 431 September 21 homework discussion

1. An element u of $\mathbf{Z}_F$ is a unit if and only if $N(u) = \pm 1$. A unit is nontrivial if it is not equal to ± 1. Find all nontrivial units in all imaginary quadratic fields. Find a nontrivial unit in $\mathbf{Q}(\sqrt{3})$. Find a nontrivial unit in $\mathbf{Q}(\sqrt{6})$. Find a nontrivial unit in $\mathbf{Q}(\sqrt{29})$.

Discussion. If $N(u) = uu' = \pm 1$ then u is a unit. On the other hand, if $uv = 1$ then $N(u)N(v) = 1$ so $N(u) = \pm 1$ since the norm of an algebraic integer is an integer.

As usual let $\delta = \sqrt{d}$, or $(1 + \sqrt{d})/2$ according as $d \equiv 2, 3 \bmod 4$ or $d \equiv 1 \bmod 4$; in the first case, the discriminant D is equal to $4d$ and the norm form is $N(x+y\delta) = x^2 - dy^2$, and in the second case $D = d$ and $N(x+y\delta) = x^2 + xy - d'y^2$ where $d' = (d-1)/4$.

If F is an imaginary quadratic field ($d < 0$) of the first type then a unit $x + y\delta$ satisfies $x^2 - dy^2 = 1$. Note that $-d$ is positive so this is a hard equation to solve; if $d < -1$ then the only solution is $x = \pm 1, y = 0$, and if $d = -1$ then there are four solutions — two as before, and $x = 0, y = \pm 1$.

If F is an imaginary quadratic field of the second type ($d \equiv 1 \bmod 4$) then we are interested in the equation

$$x^2 + xy - d'y^2 = 1.$$

(Note that since d' is negative, the RHS can not be -1.) Multiplying by 4 and completing the square shows that we are interested in

$$(2x + y)^2 - dy^2 = 4.$$

If $d = -3$ there are six solutions $x = 0, y = \pm 1$, and $2x + y = \pm 1, y = \pm 1$. If $d < -3$ then any solution has $y = 0$ so that $x = \pm 1$.

All in all we find that the units in $\mathbf{Z}_F$ for imaginary quadratic fields are as follows:

- If $D = -3$ then there are six units $\mathbf{Z}_F^* = \{\pm 1, \pm\omega, \pm\omega^2\}$, where $\omega = (-1 + \sqrt{-3})/2 = e^{2\pi i/3}$.
- If $D = -4$ then there are four units $\mathbf{Z}_F^* = \{\pm 1, \pm i\}$.
- For all other $D < 0$, $\mathbf{Z}_F^* = \{\pm 1\}$.

For real quadratic fields, we just have to find units by searching for solutions to $N(x + y\delta) = \pm 1$. For $d = 3$, one finds easily that $N(2 + \sqrt{3}) = 1$. For $d = 6$, we find $N(x + y\sqrt{6}) = x^2 - 6y^2$ and $5 + 2\sqrt{6}$ is a unit. For $d = 29$, one finds that $N(x + y\delta) = x^2 + xy - 7y^2$, and $N(2 + \delta) = -1$.

2. Let $\omega = e^{2\pi i/3} = (-1 + \sqrt{-3})/2$. Show that $\mathbf{Z}[\omega]$ is a Euclidean domain (with respect to the function $N(a + b\omega) = a^2 - ab + b^2$.) Show 5 is a prime element in $\mathbf{Z}[\omega]$ but that 3 and 7 are not. What is the order of the quotient $\mathbf{Z}[\omega]/I$ where I is the principal ideal $(1 - \omega)$. Same question for $I = (5)$.

Discussion. If x and y are elements of $\mathbf{Z}[\omega]$, with $y \neq 0$ then write $x/y = A + B\omega$, where $A, B \in \mathbf{Q}$. Let the quotient q be $a + b\omega$, where a and b are the

nearest integers to the rational number A and B respectively. Then $|a-A| \leq 1/2$, $|b-B| \leq 1/2$. Then

$$\begin{aligned} N(x-y(a+b\omega)) &= N(y)N(x/y-(a+b\omega)) \\ &= N(y)\left((A-a)^2-(A-a)(B-b)+(B-b)^2\right) \leq 3N(y)/4 < N(y) \end{aligned}$$

so $\mathbf{Z}[\omega]$ is euclidean as claimed.

The ideal $I=(1-\omega)$ contains 3 since $N(1-\omega)=3$. Since $\omega \equiv 1 \bmod I$ it follows that $a+b\omega \equiv a+b \bmod I$. Therefore every element in the ring is congruent to 0, 1, or 2 modulo I, and there are three cosets and the quotient $\mathbf{Z}[\omega]/I$ has three elements.

The ideal $I=(5)$ is of index 25. Indeed, every element $a+b\omega$ is congruent to one of the 25 elements $a+b\omega$, where $0 \leq a,b < 5$, and it is easy to check that no two of these are congruent modulo I.

3. Let p be an odd prime. Prove that $f(x)=(x^p-1)/(x-1)=x^{p-1}+x^{p-2}+\cdots+x+1$ is irreducible, so that $[\mathbf{Q}(e^{2\pi/p}):\mathbf{Q}]=p-1$. Prove that $[\mathbf{Q}(\cos(2\pi/p):\mathbf{Q}]=(p-1)/2$.

Discussion. From the binomial theorem we have

$$f(x+1)=\left((x+1)^p-1\right)/x=\sum_{i=1}^{p}\binom{p}{i}x^{i-1}$$

which is irreducible by the Eisenstein criterion. Therefore f is irreducible, and $[\mathbf{Q}(z):\mathbf{Q}]=p-1$ since f is the minimal polynomial of $z=e^{2\pi i/p}$.

The field $\mathbf{Q}(\cos(2\pi/p)$ is a subfield of $\mathbf{Q}(z)$ since $\cos(2\pi/p)=(z+z^{-1})/2$, and it is a proper subfield (since $\mathbf{Q}(\cos(2\pi/p)$ has an embedding in $\mathbf{R}$, but $\mathbf{Q}(z)$ does not). On the other hand, z satisfies a quadratic equation over the field, since $z^2-2\cos(2\pi/p)z+1=0$. Thus the degree is exactly two, and by multiplicativity of degrees we have $[\mathbf{Q}(\cos(2\pi/p):\mathbf{Q}]=(p-1)/2$.

4. Let $F=\mathbf{Q}(\sqrt{2})$. Let $u=-1+\sqrt{2}$. Prove that $\mathbf{Z}_F^*=\{\pm u^k : k \in \mathbf{Z}\}$.

Discussion. It is slightly more convenient to work with $v:=-u'=1+\sqrt{2}$ so we prove that $\mathbf{Z}_F^*=\{\pm v^k : k \in \mathbf{Z}\}$. If w is a unit then, by negating and reciprocating if necessary we can assume that $w=a+b\sqrt{2}>1$. Since $a \geq 1$ and $b \geq 1$ we see that if $w \neq v$ then $w > v$. Then w has to be a positive power of v; indeed $v^k < w < v^{k+1}$ then $1 < w/v^k < v$, but there are no units between 1 and v.

Note, for the sake of the next problem, that $uu'=-1$ so that $u^{-1}=-1/u'$, and the set of all units is the same as the set $\{\pm(1\pm\sqrt{2})^k : k \geq 0\}$.

5. Find all integers that are simultaneously triangular and square, such as 1 and 36.

Discussion. We are being asked to solve

$$y^2=\frac{x(x+1)}{2}$$

in positive integers. Multiplying by 8 and doing some algebra leads to

$$(2x+1)^2 - 2(2y)^2 = 1.$$

From the analysis in the preceding equation we know that this implies that

$$2x + 1 + 2y\sqrt{2} = \pm(3 \pm 2\sqrt{2})^n$$

for some positive integer n. (Since the unit has norm 1, we take powers of v^2 rather than v.) The right hand side has the form $\pm(A + B\sqrt{2})$ where A is positive, so the first $\pm$ sign can be eliminated. Since the RHS is less then one if the remaining sign is chosen to be positive, we see that the other sign is positive as well. Using the binomial theorem, we find that the integers that are simultaneously square and triangular are

$$y^2 = \left(\sum_{k=0}^{[(n-1)/2]} \binom{n}{2k+1} 3^{n-2k-1} 2^{3k} \right)^2 .$$

Alternatively, we can give a clean iterative description. Define a pair of sequences x_n, y_n by initial values $x_1 = 3$, $y_1 = 2$ together with a joint recursion $x_{n+1} = 3x_n + 4y_n$, $y_{n+1} = 3x_n + 2y_n$. The simultaneously square and triangular integers are numbers of the form $(y_n/2)^2$. The first few examples are $1, 36, 1225, 41616, 1413721, 48024900, \cdots$.

6. Suppose that K is an algebraic number field, and that α is integral over K in the sense that it satisfies a monic polynomial whose coefficients are in $\mathbf{Z}_K$. Prove that α is an algebraic integer.

Discussion. An algebraic number z is an algebraic integer then

$$\mathrm{spn}_{\mathbf{Z}}(1, z, z^2, \cdots)$$

has a finite basis. Each of the coefficients of the minimal polynomial of α over K is an algebraic integer, so they are all contained in a finitely generated abelian group G, and the polynomial equation of degree n for α shows that α is contained in the group generated by the first $n-1$ powers of α and the generators of G, so that α is an algebraic integer itself.