MATH 371
HOMEWORK SET 4
DUE 12.12.2012, WEDNESDAY

Remember: a, b, etc. stand for integers! p stand ALWAYS for a prime number. $\mathcal{O}_{\sqrt{\Delta}}$ stands for the ring of integers of the quadratic number field $\mathbf{Q}(\sqrt{\Delta})$. α, β etc. stand for elements of $\mathcal{O}_{\sqrt{\Delta}}$.

(1) Show that the intersection of two distinct quadratic number fields, $\mathbf{Q}(\sqrt{\Delta})$ and $\mathbf{Q}(\sqrt{\Delta'})$ is $\mathbf{Q}$.

Solution 1. Recall that Δ and Δ' have to be square-free integers. Suppose that $\alpha \in (\mathbf{Q}(\sqrt{\Delta}) \cup \mathbf{Q}(\sqrt{\Delta'})) \setminus \mathbf{Q}$. Then $\alpha \in \mathbf{Q}(\sqrt{\Delta})$ implies that there are rationals $a, b \in \mathbf{Q}$ so that $\alpha = a + b\sqrt{\Delta}$ and similarly there are rationals $c, d \in \mathbf{Q}$ so that $\alpha = c + d\sqrt{\Delta'}$. Then we have

$$a + b\sqrt{\Delta} = c + d\sqrt{\Delta} \Leftrightarrow a - c + b\sqrt{\Delta} - d\sqrt{\Delta'} = 0.$$

As $a - c$ is a rational number as well as 0, the difference $b\sqrt{\Delta} - d\sqrt{\Delta'}$ must be a rational number, hence must be equal to 0, i.e. $b\sqrt{\Delta} = d\sqrt{\Delta'}$. $d = 0$ forces b to be 0 in which case we are done. So suppose $d \neq 0$. Then we have $\frac{b}{d} = \frac{\sqrt{\Delta'}}{\sqrt{\Delta}}$. But b/d is a rational number, hence we must have $\sqrt{\Delta'}/\sqrt{\Delta} \in \mathbf{Q}$. This says $\frac{\sqrt{\Delta'}}{\sqrt{\Delta}} = \frac{f\sqrt{\delta'}}{e\sqrt{\delta}}$ for some rational integers e, f. This says that $e^2|\Delta$ and $f^2|\Delta'$, contradiction.

(2) For $\alpha \in \mathbf{Q}(\sqrt{\Delta})$, we define the *norm* of α to be the rational number

$$\alpha \cdot \overline{\alpha}.$$

Show that

i. $N(\alpha) = 0 \Leftrightarrow \alpha = 0$.
ii. $N(\alpha\beta) = N(\alpha)N(\beta)$.
iii. If $\alpha \in \mathcal{O}_{\sqrt{\Delta}}$ the $N(\alpha) \in \mathbf{Z}$. However, show the converse to this statement is false by giving three examples of non-integers whose norm is rational integer, i.e. find three elements in the set $\mathbf{Q}(\sqrt{\Delta}) \setminus \mathcal{O}_{\sqrt{\Delta}}$ whose norms are integers.

Solution 2. i. Say $N(\alpha) = 0$. Write $\alpha = a + b\sqrt{\Delta}$. Then $N(\alpha) = \alpha\overline{\alpha} = a^2 - \Delta b^2$. Assume, to the contrary, that a_o and b_o be a non-zero solution to the equation $a^2 - \Delta b^2 = 0 \Leftrightarrow a_o^2 = \Delta b_o^2$. This implies that Δ is not square-free; contradiction. Conversely, of $\alpha = 0$ then $N(\alpha) = 0\overline{0} = 0$

ii. $N(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = \alpha\beta\overline{\alpha}\overline{\beta} = (\alpha\overline{\alpha})(\beta\overline{\beta}) = N(\alpha)N(\beta)$.

iii. There are two cases. If Δ is not congruent to $1 \pmod 4$ then elements of $\mathcal{O}_{\sqrt{\Delta}}$ are of the form $\alpha = a + b\sqrt{\Delta}$ with $a, b \in \mathbf{Z}$. Hence $N(\alpha) = a^2 - \Delta b^2 \in \mathbf{Z}$. If $\Delta \equiv 1\ (4)$ then integers of $\mathbf{Q}(\sqrt{\Delta})$ are of the form $\alpha = \frac{a}{2} + \frac{b}{2}\sqrt{\Delta}$ with $a, b \in \mathbf{Z}$ and $a \equiv b\ (2)$. $N(\alpha) = \frac{1}{4}(a^2 - \Delta b^2)$. Hence it is enough to show that $a^2 - \Delta b^2 \equiv a^2 - b^2 \equiv 0\ (4)$. If a and b are even, we are done. If both are odd, then a, b are congruent to $1 \pmod 4$.

(3) Show that each of the following numbers are primes in $\mathbf{Q}(\sqrt{-5})$:

i. $3 + 2\sqrt{-5}$,
ii. 37,
iii. $1 + 2\sqrt{-5}$.

Solution 3. i. $N(3 + 2\sqrt{-5}) = (3 + 2\sqrt{-5})(3 - 2\sqrt{-5}) = 9 + 5 \cdot 4 = 29$ is a prime, hence $3 + 2\sqrt{-5}$ must be a prime by Theorem 19 of our notes.

ii. Assume that there are integers $\alpha, \beta \in \mathcal{O}_{\sqrt{\Delta}}$ with $37 = \alpha\beta$. Then $N(37) = 37 \cdot 37 = N(\alpha\beta) = N(\alpha)N(\beta)$. As 37 is a prime, we must have $N(\alpha) = 37 = N(\beta)$. Now, write $\alpha = a + b\sqrt{-5}$. Then $N(\alpha) = a^2 + 5b^2 = 37$. But this equation has no solution in rational integers. So there are no elements of $\mathcal{O}_{\sqrt{\Delta}}$ having norm 37. Hence 37 is a prime in $\sqrt{-5}$.

iii. $N(1 + 2\sqrt{-5}) = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}) = 21 = 3 \cdot 7$. Thus, if $1 + 2\sqrt{-5}$ is not a prime, then there should exist two integers α and β of norm 3 and 7. However, there are no integers in $\mathbf{Q}(\sqrt{-5})$ of norm 3 because there are no solutions to the equation $a^2 + 5b^2 = 3$. Hence $1 + \sqrt{-5}$ is a prime.

(4) Show that 2 and 3 are not primes in $\mathbf{Q}(\sqrt{6})$. (In fact, they both can be written as a product of two associate primes.)

Solution 4. $6 \equiv 2\ (4)$, hence integers in $\mathbf{Q}(\sqrt{6})$ are of the form $\alpha = a + b\sqrt{6}$ for $a, b \in \mathbf{Z}$. And $N(\alpha) = a^2 - 6b^2$. We can write 3 as $(3+\sqrt{6})(3-\sqrt{6})$ with both being primes as they have norm 3; hence 3 is not a prime. As for factoring 2, although there are no integers of norm 2 there are integers of norm -2, the reason being that the Diophantine equation $x^2 - 6y^2 = 2$ has no solutions(can you prove this?) whereas $x^2 - 6y^2 = -2$ does have infinitely many solutions! We can write $2 = (-1)(2+\sqrt{6})(2-\sqrt{6})$. As both $2+\sqrt{6}$, $2-\sqrt{6}$ have prime norms, they are primes in $\mathcal{O}_{\sqrt{6}}$.

(5) Show that there is no integer in $\mathbf{Q}(\sqrt{7})$ of norm 3 but that 3 is not a prime in $\mathbf{Q}(\sqrt{7})$.(We have seen in class that 2 is a prime in $\mathbf{Q}(\sqrt{-47})$ because there are no elements in $\mathcal{O}_{\sqrt{\Delta}}$ with norm 2.)

Solution 5. Once again $7 \equiv 3\ (4)$ integers are of the form $a + b\sqrt{7}$. Let $\alpha = a + b\sqrt{7}$ be one. Then $N(\alpha) = a^2 - 7b^2$. The equation $x^2 - 7y^2 = 3$ has no solution in $\mathbf{Z}$, because if it had one solution then we would have:

$$3 \equiv x^2 - 7y^2 = x^2\ (7).$$

Here is a list of *squares* modulo 7: 0, 1, 4, 2, 2, 4, 1. In other words, the equation $x^2 \equiv 3\ (7)$ have no solution, hence the given equation cannot have any integers solutions. Therefore, $\mathcal{O}_{\sqrt{7}}$ does not contain any element of norm 3. However, the elements $2+\sqrt{7}$ and $2-\sqrt{7}$ does have norm -3 hence they are primes, and the product $(-1)(2+\sqrt{7})(2-\sqrt{7}) = 3$, i.e. 3 is not a prime in $\mathcal{O}_{\sqrt{7}}$.

(6) Suppose that ε is a unit in $\mathbf{Q}(\sqrt{\Delta})$ and $\sqrt{\varepsilon}$ is an integer(i.e. an element of $\mathcal{O}_{\sqrt{\Delta}}$). Show that $\sqrt{\varepsilon}$ is a unit.

Solution 6. ε is a unit implies that $N(\varepsilon) = \pm 1$. As $\sqrt{\varepsilon}$ is an integer, $N(\varepsilon) = N(\sqrt{\varepsilon}\cdot\sqrt{\varepsilon}) = N(\sqrt{\varepsilon})^2 = 1$, i.e. $(N(\sqrt{\varepsilon}))^2 = 1$, hence $N(\sqrt{\varepsilon}) = \pm 1$, i.e. $\sqrt{\varepsilon}$ is a unit, by Theorem 16 of our notes.

(7) Prove that $\mathcal{O}_{\sqrt{\Delta}}$ is not a UFD for $\Delta =$:
   i. -17 (Hint: Try to factor 18 to see that the number of factors in two decompositions may be different.)
   ii. -26 (Hint: Try to factor 27 to see that the number of distinct primes appearing in two decompositions may be different.)

Solution 7. i. $18 = 2\cdot 3\cdot 3 = (1+\sqrt{-17})(1-\sqrt{-17})$. We have to show that each factor is a prime. 2 and 3 are primes because there are no integers of norm ± 2 and ± 3 in $\mathbf{Q}(\sqrt{-17})$. Indeed, $N(\alpha) = N(a + b\sqrt{-17}) = a^2 + 17b^2$, and the two Diophantine equations $x^2 + 17y^2 = \pm 2$ and $x^2 + 17y^2 = \pm 3$ have no solution. Since $N(1+\sqrt{-17}) = 18 = 2\cdot 3\cdot 3$ and there are no integers of norm 2 or 3 in $\mathcal{O}_{\sqrt{-17}}$, we conclude that $1+\sqrt{-17}$ is a prime. Similar argument works for $1-\sqrt{-17}$. And in fact, we see that $\mathcal{O}_{\sqrt{-17}}$ is NOT a UFD, and in fact, the number of prime factors in decompositions may be different!

ii. $27 = 3\cdot 3\cdot 3 = (1+\sqrt{-26})(1-\sqrt{-26})$. 3 is a prime simply because there are no integers of norm ± 3 in $\mathcal{O}_{\sqrt{-26}}$ and $1 \pm \sqrt{-26}$ is prime by more or less the same arguments made in part i.. Hence $\mathcal{O}_{\sqrt{-26}}$ is NOT a UFD. We also observe that there are cases where the number of distinct factors in a prime factorization may differ in non-UFDs.

(8) Show that 2 and 3 are primes in $\mathbf{Q}(\sqrt{10})$. (Hint: Try to compute their norms. Then reduce modulo 10.)

Solution 8. Suppose 2 is not a prime and write $2 = \alpha\beta$. We must have $N(\alpha) = N(a + b\sqrt{10}) = a^2 - 10b^2 = 2$. Then modulo 10 we have $a^2 = 2\ (10)$. Similarly, suppose 3 is not a prime and write $3 = \alpha'\beta'$. We must have $N(\alpha') = N(a' + b'\sqrt{10}) = a'^2 - 10b'^2 = 3$. Then modulo 10 we have $a^2 = 3\ (10)$. Here is a list of *squares* modulo 10: 0, 1, 4, 9, 6, 5, 6, 9, 4, 1; contradiction!

Notes: You may write your solutions in the language you find appropriate.