Algebraic number theory — Exercise sheet 3

https://www.maths.tcd.ie/~mascotn/teaching/2026/MAU34109/index.html

Version: November 11, 2026

Submit your answers in class or to neumayec@tcd.ie by Thursday November 12, 1pm.

Exercise 3.1: Ideals in a cubic field (100 pts)

Let $A(x) = x^3 - 8x + 2$, and let $K = \mathbb{Q}(\alpha)$, where α is a root of $A(x)$.
Here is a table of values of $A(x)$ which you may find useful (even though you may have to compute other values of $A(x)$ at some point...):

x	-3	-2	-1	0	1	2	3
$A(x)$	-1	10	9	2	-5	-6	5

1. (2 pts) Determine the degree $[K : \mathbb{Q}]$ of K.
2. (10 pts) Prove that $\mathbb{Z}_K = \mathbb{Z}[\alpha]$.
3. (10 pts) Which primes $p \in \mathbb{N}$ ramify in K?
4. (6 pts each) For each prime $p \in \mathbb{N}$, $p \leqslant 7$, compute explicitly the decomposition of p in K (in other words, the factorisation of (p) as a product of prime ideals). Choose a name, determine the norm, and specify generators for each of the prime ideals occurring in these decompositions.
5. (4 pts each) For each $n \in \{1, 2, 3, 4, 5, 6, 7\}$, list all the ideals $\mathfrak{a}$ of $\mathbb{Z}_K$ such that $N(\mathfrak{a}) = n$.
6. Factor the following ideals into prime ideals:
   (a) (5 pts) (α),
   (b) (7 pts) $(\alpha - 3)$,
   (c) (7 pts) $(\alpha + 2)$,
   (d) (7 pts) $(\alpha + 1)$.

   Hint: Remember that $N_{\mathbb{Q}}^K(\alpha + m) = -A(-m)$ for all $m \in \mathbb{Z}$.

Solution 3.1:

1. $A(x)$ is Eisenstein at $p = 2$, and therefore irreducible, so $A(x)$ is the minimal polynomial of α whence $[K : \mathbb{Q}] = \deg A = 3$.

2. $A(x) \in \mathbb{Z}[x]$ is monic so $\alpha \in \mathbb{Z}_K$, so $\mathbb{Z}[\alpha]$ is an order in $\mathbb{Q}(\alpha) = K$. We have $\operatorname{disc}(A) = -4 \cdot (-8)^3 - 27 \cdot 2^2 = 2^2(8^3 - 27) = 2^2(512 - 27) = 2^2 \cdot 485 = 2^2 \cdot 5 \cdot 97$ where 97 is prime, so the order $\mathbb{Z}[\alpha]$ is maximal at all p except maybe at $p = 2$. However, since $A(x)$ is Eisenstein at 2, $\mathbb{Z}[\alpha]$ is actually also maximal at $p = 2$ (and 2 is totaly ramified in K, which is not useful for now but will be useful in a later question). The result follows.

3. The primes that ramify are the ones which divide the discriminant, which in this case is $\operatorname{disc} K = -2^2 \cdot 5 \cdot 97$ as $\mathbb{Z}_K = \mathbb{Z}[\alpha]$ according to the previous question. Therefore, the primes that ramify in K are precisely 2, 5, and 97.

4. Since $\mathbb{Z}_K = \mathbb{Z}[\alpha]$, we can see how p decomposes by studying how $A(x)$ factors mod p for all p. For this, we can use the fact that since it is of degree 3, it is irreducible iff. it has no root.

   - Mod $p = 2$, we have $A(x) \equiv x^3$, whence

     $$2\mathbb{Z}_K = \mathfrak{p}_2^3, \quad \mathfrak{p}_2 = (2, \alpha), \quad N(\mathfrak{p}_2) = 2.$$

     So 2 is totally ramified, but we already knew this from the fact that $A(x)$ is Eisenstein at 2.

   - Mod $p = 3$, we spot from the table of values that $x = -1 \bmod 3$ is the only root of $A(x)$ mod 3. Therefore, $x + 1$ is a factor of $A(x)$ mod 3. An Eculidean divion mod 3 reveals that $A(x) \equiv (x + 1)(x^2 - x - 1) \bmod 3$. Since $x = -1 \bmod 3$ is the only root of $A(x)$, and since it is not a root of $x^2 - x - 1$ (not even mod 3), $x^2 - x - 1$ has no roots mod 3, and is therefore irreducible (since it has degree 2, so it would have a linear factor and hence a root if it factored). Alternatively, since we have established that 3 does not ramify in K, the factor $x^2 - x - 1$ must be irreducible mod 3, since otherwise $x + 1$ would be a repeated factor which would result in a prime above 3 being repeated, contradicting the fact that 3 does not ramify in K. Thus

     $$3\mathbb{Z}_K = \mathfrak{p}_3\mathfrak{q}_9, \quad \mathfrak{p}_3 = (3, \alpha+1), \mathfrak{q}_9 = (3, \alpha^2-\alpha-1), \quad N(\mathfrak{p}_3) = 3, N(\mathfrak{q}_9) = 9.$$

   - Mod $p = 5$, we spot from the table of values that $x = -2$ and $x = 1$ are the only roots of $A(x)$ (since $3 \equiv -2 \bmod 5$). As we know were are going to get ramification, $A(x)$ must be either $(x+2)^2(x-1)$ or $(x+2)(x-1)^2$. Since the coefficient of x^2 vanishes, the sum of the roots vanishes, so $A(x) \equiv (x + 2)(x - 1)^2$ (alternatively, we could look at the constant coefficient, or simply try to expand both possible facotisations and see which one matches). Thus

     $$5\mathbb{Z}_K = \mathfrak{p}_5\mathfrak{q}_5^2, \quad \mathfrak{p}_5 = (5, \alpha + 2), \mathfrak{q}_5 = (5, \alpha - 1), \quad N(\mathfrak{p}_5) = N(\mathfrak{q}_5) = 5.$$

- Since $-3 \cdots 3$ covers $\mathbb{Z}/7\mathbb{Z}$, we see from the table of values that $A(x)$ has no root mod 7. Since it has degree 3, it would have a linear factor and hence a root if it factored, so $A(x)$ remains irreducible mod 7. This means that 7 is inert in K: $7\mathbb{Z}_K = \mathfrak{p}_{7^3}$, where $\mathfrak{p}_{7^3} = (7)$ has norm $7^3 = 343$.

5. We examine each value of n separately.

   (a) The only ideal of norm 1 (in any number field) is $\mathbb{Z}_K$ (as an improper ideal of itself), since by definition $N(\mathfrak{a}) = [\mathbb{Z}_K : \mathfrak{a}]$. Conclusion: $\mathbb{Z}_K$.

   (b) Suppose $N(\mathfrak{a}) = 2$. The norm of a prime ideal is always a prime power, so the only possiblilty is that $\mathfrak{a}$ is itself prime, above $p = 2$ and of residue degree $f = 1$. From the decomposition of $p = 2$ established in the previous question, the only possibility is $\mathfrak{a} = \mathfrak{p}_2$. Conclusion: $\mathfrak{p}_2$.

   (c) Similarly, if $N(\mathfrak{a}) = 3$, then $\mathfrak{a}$ must be a prime above $p = 3$ with $f = 1$. The only possibility is $\mathfrak{a} = \mathfrak{p}_3$ (since $\mathfrak{q}_9$, having $f = 2$, would have norm 3^2 instead of 3^1). Conclusion: $\mathfrak{p}_3$.

   (d) The case $N(\mathfrak{a}) = 4$ is a bit more interesting: $\mathfrak{a}$ could either be a prime ideal of norm 2^2 (hence above $p = 2$ and with $f = 2$), or a product of two (not necessarily distinct) prime ideals of norm 2^1 (hence both above $p = 2$ and with $f = 1$). The decomposition of 2 shows that the first case is not possible, whereas the only possiblity for the second case is $\mathfrak{a} = \mathfrak{p}_2^2$. Conclusion: $\mathfrak{p}_2^2$.

   (e) Similarly to the cases $n = 2$ and $n = 3$, since 5 is prime, any ideal of norm 5 must be a prime above 5, with $f = 1$. However, unlike for $n = 2$ and $n = 3$, we have two choices this time: $\mathfrak{p}_5$ and $\mathfrak{q}_5$. Conclusion: $\mathfrak{p}_5$, $\mathfrak{q}_5$.

   (f) $6 = 2 \cdot 3$. Since the norm of a prime ideal must be a prime power, any ideal of norm 6 must be made up of a prime of norm 2 times a prime of norm 3. We have seen that there is only one possibility for each of these primes. Conclusion: $\mathfrak{p}_2\mathfrak{p}_3$.

   (g) Similarly to the cases $n = 2, 3, 5$, since 7 is prime, we would be looking at a prime above $p = 7$ with $f = 1$. However, the only prime above 7 has $f = 3$. Conclusion: no such ideal.

6. We know that $N((\alpha + n)) = |N_{\mathbb{Q}}^K(\alpha + n)| = |-A(-n)|$ for all $n \in \mathbb{Z}$. Thus

   - $N((\alpha)) = 2$, so $(\alpha) = \mathfrak{p}_2$ from the previous question.

     $$(\alpha + 2) = \mathfrak{p}_2.$$

   - $N((\alpha - 3)) = 5$, so $(\alpha - 3)$ is either $\mathfrak{p}_5$ or $\mathfrak{q}_5$. However, we also know that $\alpha - 3 = \alpha + 2 - 5 \in \mathfrak{p}_5 = (5, \alpha + 2)$, so $(\alpha - 3) \subseteq \mathfrak{p}_5$, so $\mathfrak{p}_5 \mid (\alpha - 3)$, which shows that $(\alpha - 3) = \mathfrak{p}_5$. Alternatively, if we had $(\alpha - 3) = \mathfrak{q}_5$, then we would have $\alpha - 3 \in \mathfrak{q}_5 = (5, \alpha - 1)$, whence $2 = (\alpha - 1) - (\alpha - 3) \in \mathfrak{q}_5$, whence $1 = 5 - 2 - 2 \in \mathfrak{q}_5$, whence $\mathfrak{q}_5 = \mathbb{Z}_K$, absurd.

- $N((\alpha+2)) = 10 = 2 \cdot 5$, so $(\alpha+2)$ must be the product of a prime of norm 2 and of a prime of norm 5 (same logic as the $n = 6$ case in the previous question), so it is either $\mathfrak{p}_2\mathfrak{p}_5$ or $\mathfrak{p}_2\mathfrak{q}_5$. Since $\alpha + 2 \in \mathfrak{p}_5$, we conclude as previously that $\mathfrak{p}_5 \mid (\alpha+2)$ (or that $\mathfrak{q}_5 \nmid (\alpha+2)$), whence $(\alpha+2) = \mathfrak{p}_2\mathfrak{p}_5$.
- $N((\alpha+1)) = 9 = 3^2$, so $(\alpha+1)$ could be either $\mathfrak{p}_3^2$ or $\mathfrak{q}_9$. However, $\mathfrak{p}_3 = (3, \alpha+1) \ni \alpha+1$, so $\mathfrak{p}_3 \mid (\alpha+1)$, so $(\alpha+1) = \mathfrak{p}_3^2$ (by uniqueness of the factorisation).

This was the only mandatory exercise, that you must submit before the deadline. The following exercises are not mandatory; they are not worth any points, and you do not have to submit them. However, I highly recommend that you try to solve them for practice (they may even give you inspiration to help you solve Exercise 1), and you are welcome to email me if you have questions about them. The solutions will be made available with the solution to the mandatory exercise.

Exercise 3.2: Ideals of fixed norm

How many ideals of norm 900 are there in the ring of integers of $\mathbb{Q}(\sqrt{7})$?
Hint: Compute the decomposition in $\mathbb{Q}(\sqrt{7})$ of the prime factors of 900.

Solution 3.2:

The key to this exercise is to remember that the norm of ideals is multiplicative, and that the norm of a prime $\mathfrak{p}$ of residual degree f above $p \in \mathbb{N}$ is p^f. Thus for instance if $\mathfrak{a}$ is an ideal of norm $200 = 2^3 5^2$, and if $\mathfrak{a}$ factors as

$$\mathfrak{a} = \prod_i \mathfrak{p}_i^{e_i},$$

then the factor 5^2 in 200 comes exclusively from the primes $\mathfrak{p}_i$ that lie above 5, and similarly for 2^3. Also, all the $\mathfrak{p}_i$ lie either above 2, or above 5, since they would contribute another prime to the norm of $\mathfrak{a}$ else. So if we regroup the $\mathfrak{p}_i$ according to the rational prime $p \in \mathbb{N}$ they lie above, say

$$\mathfrak{a} = \left(\prod_{\mathfrak{p}_i | 2} \mathfrak{p}_i^{e_i} \right) \left(\prod_{\mathfrak{p}_i | 5} \mathfrak{p}_i^{e_i} \right)$$

where $\mathfrak{p} \mid p$ means that the prime ideal $\mathfrak{p}$ lies above the prime number p, then we have $N\left(\prod_{\mathfrak{p}_i|2} \mathfrak{p}_i^{e_i}\right) = 2^3$ and $N\left(\prod_{\mathfrak{p}_i|5} \mathfrak{p}_i^{e_i}\right) = 5^2$. And then, the kind of primes $\mathfrak{p}_i$ and exponents e_i that we can use to achieve these equalities depends on how 2 and 5 decompose.

So, back to the question of the exercise, let $K = \mathbb{Q}(\sqrt{7})$. In order to find the ideals of norm $900 = 2^2 3^2 5^2$ in K, we first take a look at how 2, 3 and 5 decompose in K.

As $7 \equiv 3 \bmod 4$, we find that 2 ramifies in K, say

$$2\mathbb{Z}_K = \mathfrak{p}_2^2,$$

where $\mathfrak{p}_2$ has residual degree 1 and hence norm $2^1 = 2$. So the factor $2^2 \mid 900$, which can only come from primes above 2, must actually come from $\mathfrak{p}_2^2$, since there is no other choice.

Next, since $7 \equiv 1 \bmod 3$ is a square mod 3, we find that 3 splits in K, say

$$3\mathbb{Z}_K = \mathfrak{p}_3 \mathfrak{p}_3'.$$

This time the situation is more interesting: to make the factor $3^3 \mid 900$, we need either two primes of degree 1 above 3, or one prime of degree 2 above 3; but both $\mathfrak{p}_3$ and $\mathfrak{p}_3'$ have degree 1, so the only choices we have are to take $\mathfrak{p}_3$ twice, or $\mathfrak{p}_3'$ twice, or both $\mathfrak{p}_3$ and $\mathfrak{p}_3'$ once each.

Finally, since 7 is not a square mod 5 (as can been seen by computing $x^2 \bmod 5$ for x from 1 to 5), we find that 5 is inert in K, so that the only prime above 5 is $\mathfrak{p}_5 = 5\mathbb{Z}_K$ itself. It has degree 2, so its norm is 5^2, and so the only way of producing the factor $5^2 \mid 900$ is to take $\mathfrak{p}_5$.

To sum up, for 2 and for 5 we have only one choice, whereas for 3 we have three choices. So there are exactly three ideals of norm 900 in K, namely $\mathfrak{p}_2^2\mathfrak{p}_3^2\mathfrak{p}_5$, $\mathfrak{p}_2^2\mathfrak{p}_3'^2\mathfrak{p}_5$, and $\mathfrak{p}_2^2\mathfrak{p}_3\mathfrak{p}_3'\mathfrak{p}_5$.

Note that we can simplify these expressions a bit: since $\mathfrak{p}_2^2 = 2\mathbb{Z}_K$, $\mathfrak{p}_3\mathfrak{p}_3' = 3\mathbb{Z}_K$, and $\mathfrak{p}_5 = 5\mathbb{Z}_K$, we find that our three ideals of norm 900 are $10\mathfrak{p}_3^2$, $10\mathfrak{p}_3'^2$, and $30\mathbb{Z}_K$.

Exercise 3.3: Similar-looking yet non-isomorphic number fields

The goal of this exercise is to prove that the number fields $\mathbb{Q}(\sqrt[3]{6})$ and $\mathbb{Q}(\sqrt[3]{12})$ have the same degree and discriminant, but are not isomorphic.

To ease notation, we let $\alpha = \sqrt[3]{6}$, $\beta = \sqrt[3]{12}$, $K = \mathbb{Q}(\alpha)$ and $L = \mathbb{Q}(\beta)$.

1. Prove that $[K : \mathbb{Q}] = 3$.
2. Prove that $\mathbb{Z}_K = \mathbb{Z}[\alpha]$ and compute $\operatorname{disc} K$.
3. Prove that $[L : \mathbb{Q}] = 3$ and that $\operatorname{disc} L$ is of the form $-2^a 3^5$ for some integer $a \geqslant 0$. What are the possible values of a ?
4. Prove that $L \simeq \mathbb{Q}(\sqrt[3]{18})$.

   Hint: Take a look at $\gamma = \beta^2/2$.
5. Deduce that $\operatorname{disc} L = \operatorname{disc} K$.
6. Which primes $p \in \mathbb{N}$ ramify in K? What about L?
7. Compute explicitly the decomposition of 7 in K and in L.
8. Deduce that K and L are not isomorphic.
9. Compute explicitly the decomposition of 2 and 3 in K and in L.
10. Deduce the factorisation of the ideals $\alpha\mathbb{Z}_K$, $\beta\mathbb{Z}_L$ and $\gamma\mathbb{Z}_L$ into primes.

Solution 3.3:

1. Clearly, α is a root of the polynomial $f(x) = x^3 - 6 \in \mathbb{Z}[x]$. This polynomial is Eisenstein at 2 (and also at 3), so it is irreducible over $\mathbb{Q}$; it is therefore the minimal polynomial of α. This shows that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg f(x) = 3$.

2. Since $f(x) \in \mathbb{Z}[x]$ is monic, $\alpha \in \mathbb{Z}_K$. Also, α is a primitive element of K by definition of K, so $\mathbb{Z}[\alpha]$ is an order in K.

   The discriminant of this order is

   $$\operatorname{disc} \mathbb{Z}[\alpha] = \operatorname{disc} f = -3^3 6^2 = -2^2 3^5,$$

   so the only primes at which $\mathbb{Z}[\alpha]$ might not be maximal are 2 and 3. However, $f(x)$ is Eisenstein at 2 and 3, so $\mathbb{Z}[\alpha]$ is in fact maximal at 2 and 3, whence $\mathbb{Z}_K = \mathbb{Z}[\alpha]$, and so $\operatorname{disc} K = \operatorname{disc} \mathbb{Z}[\alpha] = -2^2 3^5$.

3. Just as in question 1, the fact that $g(x) = x^3 - 12$ is Eisenstein at 3 implies that it is irreducible, so it is the minimal polynomial of β, whence

   $$[\mathbb{Q}(\beta) : \mathbb{Q}] = \deg g(x) = 3.$$

   Next, for the same reasons as in question 2, we find that $\mathbb{Z}[\beta]$ is an order in L, of discriminant

   $$\operatorname{disc} g = -3^3 12^2 = -2^4 3^5.$$

   As a result, this order is maximal at every prime except maybe 2 and 3. Since $g(x)$ is Eisenstein at 3, this order is actually maximal at 3; however this argument does **not** apply at 2 because $2^2|12$. So all we can say is that

   $$\operatorname{disc} L = \frac{-2^4 3^5}{m^2},$$

   where m is the index of $\mathbb{Z}[\beta]$, which is thus a power of 2 (possibly $m = 1$). Thus

   $$\operatorname{disc} L = -2^a 3^5$$

   with $a \in \{0, 2, 4\}$.

4. We have $\gamma^3 = \beta^6/2^3 = 18$. Since $h(x) = x^3 - 18$ is Eisenstein at 2, it is irreducible over $\mathbb{Q}$, so $h(x)$ is the minimal polynomial both of γ and of $\sqrt[3]{18}$. This shows that the fields $\mathbb{Q}(\gamma)$ and $\mathbb{Q}(\sqrt[3]{18}$ have degree 3 and are isomorphic. As $\gamma \in L$, we deduce that L contains $\mathbb{Q}(\gamma)$, which is a copy of $\mathbb{Q}(\sqrt[3]{18})$. Actually, since both L and $\mathbb{Q}(\sqrt[3]{18})$ have degree 3, the inclusion $\mathbb{Q}(\gamma) \subset L$ is an equality, and thus

   $$L = \mathbb{Q}(\gamma) \simeq \mathbb{Q}(\sqrt[3]{18}).$$

5. Again, $\mathbb{Z}[\gamma]$ is an order in L, of discriminant

   $$\operatorname{disc} \mathbb{Z}[\gamma] = \operatorname{disc} h = -3^3 18^2 = -2^2 3^7.$$

But h is Eisenstein at 2, so as in question 3 we deduce that

$$\operatorname{disc} L = -2^2 3^b$$

with $b \in \{1, 3, 5, 7\}$ this time.

By comparing this information with what we have found in question 3, we deduce that

$$\operatorname{disc} L = -2^2 3^5 = \operatorname{disc} K.$$

(By the way, this means that neither $\mathbb{Z}[\beta]$ nor $\mathbb{Z}[\gamma]$ are maximal; in fact, we see that their respective indices are 2 and 3.)

6. The primes that ramify in K are exactly the ones that divide $\operatorname{disc} K$, that is to say 2 and 3. Since $\operatorname{disc} L = \operatorname{disc} K$, these are also the primes that ramify in L.

7. Since $\mathbb{Z}_K = \mathbb{Z}[\alpha]$, we can read the decomposition of 7 in $\mathbb{Z}_K$ off the factorisation of $f(x) \bmod 7$. In order to compute this factorisation, let us make a table of the values of $x^3 \bmod 7$, so as to look for roots of $f(x) \bmod 7$:

$x \bmod 7$	0	1	2	3	-3	-2	-1
$x^3 \bmod 7$	0	1	1	-1	1	-1	-1

As $f(x) \equiv x^3 + 1 \bmod 7$, we see that 3, -2 and -1 are roots of $f(x) \bmod 7$, whence

$$f(x) \equiv (x-3)(x+2)(x+1) \bmod 7.$$

So 7 splits completely in K, more precisely

$$7\mathbb{Z}_K = (7, \alpha - 3) \cdot (7, \alpha + 2) \cdot (7, \alpha + 1)$$

where each of the three factors is a prime ideal of $\mathbb{Z}_K$.

Let us move on to the decomposition of 7 in $\mathbb{Z}_L$. The order $\mathbb{Z}[\beta] \subset \mathbb{Z}_L$ may not be maximal, but it is maximal at 7, so we can still read the decomposition of 7 in $\mathbb{Z}_K$ off the factorisation of $g(x) \bmod 7$ (we could just as well consider $h(x)$ since $\mathbb{Z}[\gamma]$ is maximal at 7 too).

Thanks to the table above, we see that $x^3 \not\equiv 12 \bmod 7$ for all $x \in \mathbb{Z}/7\mathbb{Z}$, so $g(x)$ has no root mod 7. Since it has degree 3, this means that it is irreducible over $\mathbb{Z}/7\mathbb{Z}$ (because else it would have at least one linear factor). As a consequence, 7 is inert in $\mathbb{Z}_L$, i.e.

$$7\mathbb{Z}_L$$

is a prime ideal (of degree 3) of $\mathbb{Z}_L$.

8. That's because the splitting behaviour of 7 is not the same in K and L: by the previous question, 7 splits completely in K, but not at all in L.

9. For K, this is easy. Indeed, the fact that $\mathbb{Z}_K = \mathbb{Z}[\alpha]$ implies that we can compute the decomposition of any prime p (in particular 2 and 3) by factoring $f(x) \bmod p$.

   As $f(x) \equiv x^3 \bmod 2$, we have
   $$2\mathbb{Z}_K = \mathfrak{p}_2^3$$
   where $\mathfrak{p}_2 = (2, \alpha) \subset \mathbb{Z}_K$ is a prime ideal. Also, $f(x) \equiv x^3 \bmod 3$, so
   $$3\mathbb{Z}_K = \mathfrak{p}_3^3$$
   where $\mathfrak{p}_3 = (3, \alpha) \subset \mathbb{Z}_K$ is another prime ideal.

   In particular, both 2 and 3 are totally ramified in K. We already knew that they are ramified from question 6, and in fact we already knew that they are totally ramified because $f(x)$ is Eisenstein at 2 and 3.

   Let us now deal with L. Here things are a bit more complicated since we do not know a nice form for $\mathbb{Z}_L$ (it is not too difficult to prove that $\mathbb{Z}_L = \mathbb{Z}[\beta, \gamma] = \mathbb{Z} \oplus \mathbb{Z}\beta \oplus \mathbb{Z}\gamma$, but this does not help to compute how primes decompose in L).

   So, for $p = 2$, we cannot read the decomposition of 2 off the factorisation of $g(x) \bmod 2$ because $\mathbb{Z}[\beta]$ is unfortunately not maximal at 2 (or, at least, we do not know if it is). But $\mathbb{Z}[\gamma]$ is ! So we can use $h(x)$ instead. We have $h(x) \equiv x^3 \bmod 2$, whence
   $$2\mathbb{Z}_L = \mathfrak{q}_2^3,$$
   where $\mathfrak{q}_2$ is the prime ideal $(2, \gamma)$ of $\mathbb{Z}_L$. Similarly, for $p = 3$ we must not use $h(x)$, but we can use $g(x)$, and since $g(x) \equiv x^3 \bmod 3$, we have
   $$3\mathbb{Z}_L = \mathfrak{q}_3^3,$$
   where $\mathfrak{q}_3$ is the prime ideal $(3, \beta)$ of $\mathbb{Z}_L$.

   So again 2 and 3 are both totally ramified in L (even though K and L are not isomorphic, as we now know). And again, we already knew this: for 2, is it because $h(x)$ is Eisenstein at 2, and for 3, it is because $g(x)$ is Eisenstein at 3.

10. We know that the norm of the ideal $\alpha\mathbb{Z}_K$ is $|N_{\mathbb{Q}}^K(\alpha)| = 6 = 2 \cdot 3$ (because $x^3 - 6$ is in fact the characteristic polynomial of α as it has the same degree as $[K : \mathbb{Q}]$, and the determinant of a matrix is up to sign the constant coefficient of its characteristic polynomial). So this ideal must be the product of a prime of degree 1 above 2 and of a prime of degree 1 above 3. Luckily, we have just seen that there is only one prime above 2 and one prime above 3 in $\mathbb{Z}_K$, so necessarily
    $$\alpha\mathbb{Z}_K = \mathfrak{p}_2\mathfrak{p}_3.$$

    Next, the norm of $\beta\mathbb{Z}_L$ is $|N_{\mathbb{Q}}^L(\beta)| = 12 = 2^2 \cdot 3$, which means that this ideal is the product of a prime of degree 1 above 3 and of either two primes of degree 1 above 2 (possibly twice the same), or of one prime of degree 2 above 2. But

again, we are in luck, as there are only one prime above 2 and one prime above 3 in $\mathbb{Z}_L$. So we must have

$$\beta\mathbb{Z}_L = \mathfrak{q}_2^2\mathfrak{q}_3.$$

Similarly, $\gamma\mathbb{Z}_L$ has norm 18, and so

$$\gamma\mathbb{Z}_L = \mathfrak{q}_2\mathfrak{q}_3^3.$$

Exercise 3.4: A necessarily complicated ring of integers

Let K be a number field such that $[K : \mathbb{Q}] = 3$, and suppose[1] that $p = 2$ is totally split in K. Prove that $\mathbb{Z}_K$ is *not* of the form $\mathbb{Z}[\alpha]$ for any $\alpha \in K$.

Solution 3.4:

By contradiction, suppose we had $\alpha \in K$ such that $\mathbb{Z}[\alpha] = \mathbb{Z}_K$. Then $\alpha \in \mathbb{Z}[\alpha]$ would lie in $\mathbb{Z}_K$, and would satisfy $K = \mathbb{Q}(\alpha)$ (since $\mathbb{Z}[\alpha]$ wouldn't even be an order in K otherwise).

Since $2 \nmid [\mathbb{Z}_K : \mathbb{Z}[\alpha]] = [\mathbb{Z}_K : \mathbb{Z}_K] = 1$, Dedekind's theorem ensures that we would be able to relate the decomposition of $p = 2$ in K to the factorisation of the minimal polynomial $m_\alpha(x) \in \mathbb{Z}[x]$ mod 2. This polynomial has degree $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [K : \mathbb{Q}] = 3$, and the fact that 2 is totally split in K would mean that it factors mod 2 as a product of linear factors, which must be pairwise distinct mod 2 since otherwise this would mean ramification, not total splitting. But this is a problem: we need $\deg m_\alpha = 3$ distinct linear factors mod 2, but the only possible linear factors mod 2 are x and $x + 1 = x - 1$.

This contradiction shows that we cannot have $\mathbb{Z}_K = \mathbb{Z}[\alpha]$. More specifically, it shows that for all $\alpha \in \mathbb{Z}_K$, either $\mathbb{Q}(\alpha) \subsetneq K$ so $\mathbb{Z}[\alpha]$ is not even an order, or $\mathbb{Q}(\alpha) = K$ so $\mathbb{Z}[\alpha]$ is an order in K, but then necessarily $2 \mid [\mathbb{Z}_K : \mathbb{Z}[\alpha]]$ since Dedekind's theorem would apply otherwise.

[1] This can really happen, e.g. $K = \mathbb{Q}(\alpha)$ where $\alpha^3 - \alpha^2 - 2\alpha - 8 = 0$.