Algebraic number theory
Solutions to exercise sheet for chapter 3

Nicolas Mascot (n.a.v.mascot@warwick.ac.uk)
Aurel Page (a.r.page@warwick.ac.uk)
TA: Pedro Lemos (lemos.pj@gmail.com)

Version: March 2, 2017

Exercise 1

Let $K = \mathbb{Q}(\alpha)$, where $\alpha^3 - 5\alpha + 5 = 0$.

1. *Compute the ring of integers $\mathbb{Z}_K$ of K.*

   Let $A(x) = x^3 - 5x + 5$. We have $\operatorname{disc}(A) = -4 \cdot (-5)^3 - 27 \cdot 5^2 = 5^2 \cdot (4 \cdot 5 - 27) = -5^2 \cdot 7$, so the order $\mathbb{Z}[\alpha]$ is maximal at all p except maybe at $p = 5$. However, $A(x)$ is Eisenstein at 5 (which, by the way, proves that it is irreducible and so that K is a number field), so $\mathbb{Z}[\alpha]$ is in fact also maximal at 5. As a result,

   $$\mathbb{Z}_K = \mathbb{Z}[\alpha].$$

2. *Which primes $p \in \mathbb{N}$ ramify in K ?*

   The primes that ramify are the ones which divide the discriminant, which in this case is $\operatorname{disc} K = -5^2 \cdot 7$ according to the previous question. Therefore, the primes that ramify in K are precisely 5 and 7.

3. *For $n \in \mathbb{N}$, $n \leqslant 7$, compute explicitly the decomposition of $n\mathbb{Z}_K$ as a product of prime ideals.*

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

   - We have $1\mathbb{Z}_K = \mathbb{Z}_K$.
   - Since $A(0) \equiv A(1) \equiv 1 \bmod 2$, $A(x)$ is irreducible mod 2, and so 2 is inert in K, i.e. $2\mathbb{Z}_K = \mathfrak{p}_2$ is a prime of inertial degree 3.

- Mod 3, we have $A(-1) \equiv 0$, so $x+1 \mid A(x) \bmod 3$. After a Euclidian division, we find that $A(x) \equiv (x+1)(x^2-x-1) \bmod 3$, and the quadratic factor has no root in $\mathbb{F}_3$ so this is the full factorisation. Therefore, $3\mathbb{Z}_K = \mathfrak{p}_3\mathfrak{p}_3'$, with $\mathfrak{p}_3 = (3, \alpha+1)$ and $\mathfrak{p}_3' = (3, \alpha^2-\alpha-1)$, whose respective inertial degrees are 1 and 2.
- We have $4\mathbb{Z}_K = 2\mathbb{Z}_K \cdot 2\mathbb{Z}_K = \mathfrak{p}_2^2$.
- We have $A(x) \equiv x^3 \bmod 5$, and so $5\mathbb{Z}_K = \mathfrak{p}_5^3$, where $\mathfrak{p}_5 = (5, \alpha)$, whose inertial degree is 1. In particular, 5 is totally ramified in K, but we already knew that since $f(X)$ is Eisenstein at 5.
- We have $6\mathbb{Z}_K = 2\mathbb{Z}_K \cdot 3\mathbb{Z}_K = \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_3'$.
- Finally, we check that $A(x)$ has two roots in $\mathbb{F}_7$, namely $4 \equiv -3$ and $5 \equiv -2$, so $(x+3)(x+2) \mid f(x) \bmod 7$. A Euclidian division[1] reveals that in fact, $A(x) \equiv (x+2)^2(x+3) \bmod 7$, and so $7\mathbb{Z}_K = \mathfrak{p}_7^2\mathfrak{p}_7'$, where $\mathfrak{p}_7 = (7, \alpha+2)$ and $\mathfrak{p}_7' = (7, \alpha+3)$ both have inertial degree 1.

4. *Prove that the prime(s) above* 5 *are principal, and find explicitly a generator for them.*

   The only prime above 5 is $\mathfrak{p}_5$. We have $\alpha \in \mathfrak{p}_5$, and $N_{\mathbb{Q}}^K(\alpha) = -5$ (from the constant coefficient of $A(x)$), so $|N_{\mathbb{Q}}^K(\alpha)| = N(\mathfrak{p}_5)$, which proves that $\mathfrak{p}_5 = \alpha\mathbb{Z}_K$ is the ideal generated by α.

5. *List the ideals* $\mathfrak{a}$ *of* $\mathbb{Z}_K$ *such that* $N(\mathfrak{a}) \leqslant 7$.

   - The only ideal of norm 1 is $\mathbb{Z}_K$ itself.
   - An ideal of norm 2 would be a prime (since its norm is prime) lying above 2, but $N(\mathfrak{p}_2) = 2^3 = 8$, so no such ideal exists.
   - For the same reason, we find that the only ideal of norm 3 is $\mathfrak{p}_3$.
   - An ideal of norm 4 would be a product of ideals above 2, but since $N(\mathfrak{p}_2) = 8$, there are no such ideals.
   - An ideal of norm 5 must be a prime above 5, so must be $\mathfrak{p}_5$.
   - An ideal of norm 6 must factor as a product of primes above 2 and 3. Among these primes, the product of those lying above 2 must be of norm 2, but $N(\mathfrak{p}_2) = 8$, so there is not such ideal.
   - Finally, for the same reasons as above, the only ideals of norm 7 are $\mathfrak{p}_7$ and $\mathfrak{p}_7'$.

   As a conclusion, the ideals of $\mathbb{Z}_K$ of norm up to 7 are $\mathfrak{p}_3$, $\mathfrak{p}_5$, $\mathfrak{p}_7$ and $\mathfrak{p}_7'$.

[1] Other possibility : since -3 and -2 are the only roots of $A(x)$ mod 7, we must have either $A(x) \equiv (x+2)^2(x+3)$ or $(x+2)(x+3)^2 \bmod 7$. Expand both and check that only the first one works mod 7. (It was impossible that both would work mod 7, because $\mathbb{F}_7[x]$ is a UFD since $\mathbb{F}_7$ is a field, so we could predict that this method would succeed before we even tried.)

6. *Compute and factor explicitly the different of K.*

   Since $\mathbb{Z}_K = \mathbb{Z}[\alpha]$, the different is

   $$\mathcal{D}_K = f'(\alpha)\mathbb{Z}_K = (3\alpha^2 - 5).$$

   Besides, its norm is $|\operatorname{disc} K| = 5^2 \cdot 7$, and its prime factors are precisely the ramified primes, namely $\mathfrak{p}_5$ and $\mathfrak{p}_7$. Besides, $\mathfrak{p}_5$ and $\mathfrak{p}_7$ both have inertial degree 1, so $N(\mathfrak{p}_5) = 5^1$ and $N(\mathfrak{p}_7) = 7^1$. We can then use the fact that the norm of ideals is multiplicative to determine the exponents of $\mathfrak{p}_5$ and $\mathfrak{p}_7$ in the factorisation of $\mathcal{D}_K$:

   $$\mathcal{D}_K = \mathfrak{p}_5^2\mathfrak{p}_7.$$

Exercise 2

Let $K = \mathbb{Q}(\zeta)$, where ζ is a primitive 90^{th} root of 1.

1. *What is the degree of K ?*

   The degree of the cyclotomic field K is

   $$[K : \mathbb{Q}] = \varphi(90) = 90\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 24.$$

2. *Which primes $p \in \mathbb{N}$ ramify in K ?*

   In general, the primes that ramify in the N^{th} cyclotomic field are the ones that divide N, except for 2 which ramifies iff. $4 \mid N$. Here, $N = 90$, so 2 does **NOT** ramify in K although $2 \mid 90$. Therefore, the primes that ramify in K are 3 and 5.

3. *For $p = 2, 3, 5, 7$, describe how p decomposes in K.*

   This is just an application of theorem 3.10.1 from the notes. For each p, write $90 = p^v m$, where v is a nonnegative integer and $m \in \mathbb{N}$ is coprime to p.

   - For $p = 2$, we have $v = 1$ and $m = 45$, so the ramification indices of the primes are $\varphi(2^1) = 1$ (and so 2 is unramified, but we already knew that), their inertial degrees are the order of 2 in $(\mathbb{Z}/45\mathbb{Z})^*$ which is 12, and there are $\frac{24}{1\cdot 12} = 2$ of them. Thus

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

     splits into a product of 2 distinct unramified primes of inertial degrees 12.
   - For $p = 3$, we have $v = 2$ and $m = 10$, so the ramification indices of the primes are $\varphi(3^2) = 6$ (and so 3 is ramified, but we already knew that), their inertial degrees are the order of 3 in $(\mathbb{Z}/10\mathbb{Z})^*$ which is 4, and there are $\frac{24}{6\cdot 4} = 1$ of them. Thus

     $$3\mathbb{Z}_K = \mathfrak{p}_3^6$$

     is the 6^{th} power of a single prime (whose ramification index is thus 6) of inertial degree 4.

- For $p = 5$, we have $v = 1$ and $m = 18$, so the ramification indices of the primes are $\varphi(5^1) = 4$ (and so 5 is ramified, but we already knew that), their inertial degrees are the order of 5 in $(\mathbb{Z}/18\mathbb{Z})^*$ which is 6, and there are $\frac{24}{4\cdot 6} = 1$ of them. Thus
$$5\mathbb{Z}_K = \mathfrak{p}_5^4$$
is the 4^{th} power of a single prime (whose ramification index is thus 4) of inertial degree 6.
- Finally, for $p = 7$, we have $v = 0$ and $m = 90$, so the ramification indices of the primes are $\varphi(7^0) = 1$ (and so 7 is unramified, but we already knew that), their inertial degrees are the order of 7 in $(\mathbb{Z}/90\mathbb{Z})^*$ which is 12, and there are $\frac{24}{1\cdot 12} = 2$ of them. Thus
$$7\mathbb{Z}_K = \mathfrak{p}_7\mathfrak{p}_7'$$
splits into a product of 2 distinct unramified primes of inertial degrees 12.

4. *Give an example of a prime $p \in \mathbb{N}$ which splits completely in K.*

   The primes $p \in \mathbb{N}$ that split totally in K are the ones such that $p \equiv 1 \bmod 90$. Of course, 1 is not prime, and neither is $91 = 7 \cdot 13$ (although I'll grant you that it looks like it at the first glance), but 181 is. Thus, $p = 181$ is a (in fact, the smallest) prime which splits totally in K.

5. *Does there exist a prime $p \in \mathbb{N}$ which is inert in K ?*

   Such a p would have to be distinct from 3 and 5 (so as not to ramify) and to have order $[K : \mathbb{Q}] = 24$ in $(\mathbb{Z}/90\mathbb{Z})^*$. However, Chinese remainders tell us that
$$(\mathbb{Z}/90\mathbb{Z})^* \simeq (\mathbb{Z}/2\mathbb{Z})^* \times (\mathbb{Z}/3^2\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^* \simeq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$$
   is not cyclic (because 6 and 4 are not coprime), and so this group, which is of order 24, does not have elements of order 24. Therefore, such a p cannot exist.

   Remark: As $\mathbb{Z}_K = \mathbb{Z}[\zeta]$, this means that although the cyclotomic polynomial $\Phi_{90}(x)$ is irreducible over $\mathbb{Z}$ and $\mathbb{Q}$, it becomes reducible mod p for all $p \in \mathbb{N}$. This shows that it is not always possible to prove the irreducibility of a polynomial over $\mathbb{Q}$ by finding a prime modulo which it is irreducible.

UNASSESSED QUESTION

Exercise 3

Let K be a number field of degree n. Prove that if there exists a prime $p < n$ which splits completely in K, then $\mathbb{Z}_K$ is not of the form $\mathbb{Z}[\alpha]$ for any $\alpha \in K$.

Suppose on the contrary that $\mathbb{Z}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in K$. Then in particular α lies in $\mathbb{Z}_K$ and is a primitive element, so its minimal polynomial $A(x)$ has degree n and lies in $\mathbb{Z}[x]$. Besides, if p splits completely in K, then $A(x)$ must split into distinct n linear factors mod p, but this is not possible if $p < n$, since there are only p possibilities for these linear factors, namely $x, x+1, \cdots, x+p-1$.

In fact, this proves not only that $\mathbb{Z}[\alpha]$ is never the whole of $\mathbb{Z}_K$, but also that its index is in fact always divisible by p (i.e. it is never maximal at p).