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)
TAs: Chris Birkbeck (c.d.birkbeck@warwick.ac.uk),

George Turcas(g.c.turcas@warwick.ac.uk)

Version: February 20, 2017

Exercise 1 (40 points)

1. (20 points) *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 primes* $p \in \mathbb{N}$ *that divide 900.*

   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 inertial 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

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

   where $\mathfrak{p} \mid p$ means that the prime ideal $\mathfrak{p}$ lies above the prime number p, then we have $N\left(\prod_{\mathfrak{p}_i \mid 2} \mathfrak{p}_i^{e_i}\right) = 2^3$ and $N\left(\prod_{\mathfrak{p}_i \mid 5} \mathfrak{p}_i^{e_i}\right) = 5^2$. 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 inertial 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 $30\mathbb{Z}_K$.

2. (20 points) *How many ideals of norm* 80 *are there in the ring of integers of* $\mathbb{Q}(\zeta)$*, where* ζ *is a primitive* 60*th root of unity ?*

   Same principle. First, 80 is $2^4 5$, so we must study how 2 and 5 decompose in $L = \mathbb{Q}(\zeta)$. This is a number field of degree

   $$d = \varphi(60) = 60 \cdot (1 - 1/2) \cdot (1 - 1/3) \cdot (1 - 1/5) = 16,$$

   but fortunately we have a theorem that tells us exactly how primes decompose in this field.

   Namely, for $p = 2$ we write $60 = 2^2 \cdot 15$, which shows us that the ramification index of the primes above 2 in L is $e = \varphi(2^2) = 2$, and then we compute $2^i \bmod 15$ for $i = 1, 2, 3, \cdots$. We find $2, 4, 8$, and then 1, so the multiplicative order of 2 mod 15 is $f = 4$, so that the primes above 2 in L have inertial degree $f = 4$. So there must be $d/ef = 2$ such primes, whence

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

where both $\mathfrak{p}_2$ and $\mathfrak{p}_2$ are prime ideals of norm $p^f = 2^4$. This is precisely the factor of 80 that we want to contribute to with these primes, so we have two ways to do so: either take $\mathfrak{p}_2$ or $\mathfrak{p}_2'$.

Next, for $p = 5$, we write $60 = 5^1 \cdot 12$, so the ramification index of the primes above 5 is $e = \varphi(5^1) = 4$, and compute the powers of 5 mod 12. Since $5^2 \equiv 1 \mod 12$, the inertial degree of the primes above 5 is $f = 2$. Finally, there are $g = d/ef = 2$ of them, whence

$$5\mathbb{Z}_L = \mathfrak{p}_5^4 \mathfrak{p}_5'^4$$

where each factor has norm $p^f = 5^2$. But... but this means that there is no way to contribute only for $5^1 \mid 80$! So there are actually no ideals of norm 80 in $\mathbb{Z}_L$, just because of that.

Actually, with the benefit of hindsight, we could have stopped the computation as soon as we had noticed that the multiplicative order of 5 mod 12 is strictly greater than the exponent of 5 in 80, that is to say 1. We didn't even have to compute how 2 decomposes in L, since we already have an obstruction with the prime 5.

Exercise 2 (60 points)

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. (3 points) *Prove that* $[K : \mathbb{Q}] = 3$.

   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. (8 points) *Prove that* $\mathbb{Z}_K = \mathbb{Z}[\alpha]$ *and compute* $\operatorname{disc} K$.

   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. (10 points) *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 *?*

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. (4 points) *Prove that* $L \simeq \mathbb{Q}(\sqrt[3]{18})$. *Hint: Take a look at* $\gamma = \beta^2/2$.

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. (7 points) *Deduce that* $\operatorname{disc} L = \operatorname{disc} K$.

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. (2 points) *Which primes $p \in \mathbb{N}$ ramify in K? What about L?*

   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. (8 points) *Compute explicitly the decomposition of 7 in K and in L.*

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

x mod 7	0	1	2	3	-3	-2	-1
x^3 mod 7	0	1	1	-1	1	-1	-1

   As $f(x) \equiv x^3 + 1$ mod 7, we see that 3, -2 and -1 are roots of $f(x)$ mod 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 $g(x)$ mod 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 $x^3 \not\equiv 12$ mod 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. (3 points) *Deduce that K and L are not isomorphic.*

   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. (6 points) *Compute explicitly the decomposition of 2 and 3 in K and in L.*

   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 $f(x)$ mod p.

   As $f(x) \equiv x^3$ mod 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. (9 points) *Deduce the factorisation of the ideals $\alpha\mathbb{Z}_K$, $\beta\mathbb{Z}_L$ and $\gamma\mathbb{Z}_L$ into primes.*

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

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

UNASSESSED QUESTIONS

The next questions are not worth any points. I still recommend you to try to solve them, for practice. Correction will be available online, just as for the marked questions.

Exercise 3

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 $A(0) \equiv A(1) \equiv 1 \bmod 2$, $A(x)$ has not root mod 2, so it 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 $\mathbb{Z}_K$ itself, $\mathfrak{p}_3$, $\mathfrak{p}_5$, $\mathfrak{p}_7$ and $\mathfrak{p}_7'$.

[1] Other possibility : since -3 and -2 are the only roots of $A(x) \bmod 7$, 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.)