TATA55 HT2023

Hand-in exam batch 6

Jan Snellman

January 25, 2024

1 Exercises

1. Let $K = \mathbb{Q}(a)$, where a is a root of $a^3 = 2$. Let $L = K(b)$, where b is a root of $b^2 = -3$.

   (a) Find the minimal polynomial of a/b over K, and over $\mathbb{Q}$

   (b) Same for $a + b$

   (c) What is $[L : Q]$?

   Solution:

   (a) By writing $1, a/b, (a/b)^2$ using the basis $1, b$ for L as a K-vector space, we find linear relations between the coefficent vectors and get that $x^2 + 1/3 * a^2$ is the minimal polynomial for a/b over K. If we instead use the basis $1, a, a^2, b, ab, a^2b$ for L as a $\mathbb{Q}$-vector space, we get that $x^6 + 4/27$ is the minimal polynomial over $\mathbb{Q}$.
   Alternatively: $(a/b)^6 = -4/27$, so the minimal polynomial over $\mathbb{Q}$ divides $x^6 + 4/27$. But $27x^6 + 4$ is irreducible, hence so is $x^6 + 4/27$. Similarly, $(a/b)^2 = -a^2/3$ so the minimal polynomial over $\mathbb{Q}(a)$ divides $x^2 + a^2/3$. This polynomial has no zeroes in $\mathbb{Q}(a)$, hence it is irreducible.

   (b) $x^2 - 2 * a * x + a^2 + 3$ over K and

   $$x^6 + 9 * x^4 - 4 * x^3 + 27 * x^2 + 36 * x + 31$$

   over $\mathbb{Q}$.
   We can show this by first proving that $\mathbb{Q}(a + b) = \mathbb{Q}(a, b)$. Put $u = a + b$, then $a = u - b$ so

   $$2 = a^3 = (u - b)^3 = u^3 - 3u^2b + 3ub^2 + b^3 = u^3 - 3u^2b - 9u - 4b$$

   hence

   $$2 - u^3 - 9u = b(-3u^2 - 4)$$

from which we get that $b \in \mathbb{Q}(u)$. Then $a \in \mathbb{Q}(u)$, as well.
Since $[\mathbb{Q}(a,b) : \mathbb{Q}] = [\mathbb{Q}(a,b) : \mathbb{Q}(a)][\mathbb{Q}(a) : \mathbb{Q}] = 3 * 2 = 6$, the minimal polynomial of u over must have degree 6. Hence, the relation

$$(2 - u^3 - 9u)^2 = (b(-3u^2 - 4))^2 = -3(-3u^2 - 4)^2$$

yields the minimal polynomial over $\mathbb{Q}$.
Over $\mathbb{Q}(a)$ we use that

$$-3 = b^2 = (u - a)^2 = u^2 - 2a + a^2$$

(c) $[K : \mathbb{Q}] = 3$ and $b \notin K$, so $[L : K] = 2$. Hence, by the tower theorem, $[L : \mathbb{Q}] = 6$.

2. Let $f(x) = x^4 + x^2 + x + 1 \in \mathbb{Z}_3[x]$.

(a) Show that f is irreducible over $\mathbb{Z}_3$, then factor f over $K = \frac{\mathbb{Z}_3[x]}{(f(x))}$

(b) Consider the element $a = x + (f(x)) \in K$. What is its (multiplicative) order? Does it generate K^*?

(c) Find a generator of K^*.

Solution:

(a) f has no zeroes over $\mathbb{Z}_3$, easy check. It can not be factored as

$$x^4 + x^2 + x + 1 = (x^2 + c_1x + c_0)(x^2 + d_1x + d_2).$$

To see this, equate coefficients for like powers of x, and show that the resulting linear system of equations is not solvable. Hence, f is irreducible.
We put $K = \mathbb{Z}_3(a)$ with a satisfying the relation $a^4 = -a^2 - a - 1$. Then $(x - a)$ must divide f; in fact, f must split in K. Indeed, we see that (recall that $2 = -1$)

$$f = (x+2*a)*(x+2*a^2+2*a+1)*(x+a^3+a^2+2*a+2)*(x+2*a^3)$$

(b) Since $|K^*| = 3^4 - 1 = 80$, the order of a is a divisor of $80 = 2^4 * 5$, so 1,2,4,5,8,10,16,20,40, or 80. Using the relation $a^4 = -a^2 - a - 1$, and calculating powers of a, we see that the order of a is 40. Hence, a is not a generator of the cyclic group K^*.

(c) There are $\phi(80) = 32$ generators of K^*, so picking an element at random and checking its multiplicative order has a good chance of working. A better method is to chose an element b with $b^2 = a$. One such is $b = a^2 + a^3$.

3. Find the splitting fields of the following polynomials. Factor the polynomial in this field, and find the degree of the extension. Prove all your results in excruciating detail! The best way to ensure correctness is to construct a tower of Kronecker extensions.

   (a) $f(x) = x^3 + 2x^2 + 3x + 1 \in \mathbb{Q}[x]$
   (b) $g(x) = x^3 + 2x^2 + 3x + 1 \in \mathbb{Z}_7[x]$
   (c) $h(x) = x^3 + 2x^2 + 3x + 1 \in \mathbb{Z}_{13}[x]$

   Solution:

   (a) The polynomial f has no rational zeroes, since such a zero would have to be 1 or -1, by the rational root theorem.
   We thus put $K = \mathbb{Q}(b) = \frac{\mathbb{Q}[x]}{(x^3+2x^2+3x+1)}$. Then f factors in $K[x]$ as
   $$(x - b) * (x^2 + (b + 2) * x + b^2 + 2 * b + 3)$$
   The latter factor has no zeroes in K, hence it is irreducible. We can alternatively think as follows: the original polynomial f has a single real zero r, and K is isomorphic to $\mathbb{Q}(r) \subset \mathbb{R}$. The complex zeroes are as yet uncaptured.
   We need to go on; we put
   $$L = K[x]/(x^2 + (b + 2) * x + b^2 + 2 * b + 3) = K(c).$$
   Then f splits over L:
   $$f = (x + c + b + 2) * (x - c) * (x - b).$$
   We get that the degree of the splitting field is
   $$[L : \mathbb{Q}] = [L : K][K : \mathbb{Q}] = 2 * 3 = 6.$$

   (b) Over $\mathbb{Z}_7$ we have that $f(1) = 0$, so $x - 1$ is a factor; indeed
   $$f = (x + 6)(x^2 + 3 * x + 6)$$
   Hence, the splitting field is $\mathbb{Z}_7[x]/(x^2 + 3x + 6) = \mathbb{Z}_7(c)$, over which f splits as
   $$f = (x + 6) * (x + c + 3) * (x + 6 * c)$$
   The splitting field has degree 2 over the prime subfield.

   (c) f has no zeroes in $\mathbb{Z}_{13}$, so since it has degree 3 it is irreducible. We form
   $$K = \mathbb{Z}_{13}[x]/(x^3 + 3x + 6) = \mathbb{Z}_{13}(c)$$
   and factor f as
   $$f = (x + 12 * c) * (x + 2 * c^2 + 2) * (x + 11 * c^2 + c)$$
   So K is the splitting field; it has degree 3 over the prime subfield.

4. Let n be a positive integer, and let M_n be the set of $n \times n$-matrices with entries in $\mathbb{Z}_3$. Let G_n denote the subset of invertible matrices.

   (a) Calculate $|M_n|$ and $|G_n|$.

   (b) Calculate the number of matrices in M_n and in G_n with determinant $[2]_3$.

   (c) Calculate the fraction $\frac{|G_n|}{|M_n|}$.

   Solution: Obviously M_n has $3^{(n^2)}$ elements. A matrix is in G_n if its first row is non-zero, $3^n - 1$ choices, the second row is not parallell with the first, $3^n - 3$ choices, and so on; the k'th row must not lie in the span of the $k-1$ previous rows, so there are $3^n - 3^{k-1}$ valid choices. Hence,

$$|G_n| = \prod_{k=1}^{n} (3^n - 3^{k-1}).$$

   An invertible matrix has determinant $[1]_3$ or $[2]_3$. The map that exchanges the first and second row of an invertible matrix is a bijection on G_n which changes the sign of the determinant. This shows that there are as many matrices in G_n with determinant 1 as with determinant -1, in other words, $|G_n|/2$ of each. Of course, every matrix in M_n with determinant -1 is in G_n, so there are $|G_n|/2$ of these, as well.

   Finally, we calculate

$$\begin{aligned}
\frac{G_n}{M_n} &= 3^{-(n^2)} \prod_{k=1}^{n} (3^n - 3^{k-1}) \\
&= \prod_{k=1}^{n} 3^{-n} \prod_{k=1}^{n} (3^n - 3^{k-1}) \\
&= \prod_{k=1}^{n} (1 - 3^{k-1-n}) \\
&= \prod_{\ell=1}^{n} (1 - 3^{-\ell})
\end{aligned}$$

   This is a Pochhammar symbol, which approaches the limit

$$\prod_{\ell=1}^{n} (1 - 3^{-\ell}) \approx 0.5601$$

   which is an evaluation of Euler's function, see for instance Wikipedia.