Master Training Program : Royal Academy of Cambodia/CIMPA

Solution of the control of October 26, 2006

update: 30/10/2006

Statement

1. Recall that the continued fraction expansion of a real irrational number t, namely

$$t = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}}}$$

with $a_j \in \mathbf{Z}$ for all $j \geq 0$ and $a_j \geq 1$ for $j \geq 1$, is denoted by $[a_0;\, a_1,\, a_2,\, a_3,\, \ldots]$.

Let t be the real number whose continued fraction expansion is $[1;\, 3,\, 1,\, 3,\, 1,\, 3,\, 1, \ldots]$, which means $a_{2n} = 1$ and $a_{2n+1} = 3$ for $n \geq 0$. Write a quadratic polynomial with rational coefficients vanishing at t.

Solution

The number t satisfies

$$t = 1 + \cfrac{1}{3 + \cfrac{1}{t}}\cdot$$

An easy computation shows that t is a root of the polynomial $3X^2 - 3X - 1$.

Statement

2. Solve the equation $y^2 - y = x^2$

a) in $\mathbf{Z} \times \mathbf{Z}$,

b) in $\mathbf{Q} \times \mathbf{Q}$.

Solution

a) There are two obvious solutions $(x, y) = (0, 0)$ and $(x, y) = (0, 1)$. If there were another solution in $\mathbf{Z} \times \mathbf{Z}$, this solution would satisfy $x^2 \geq 1$ and $|y| \geq 2$. In this case the two positive integers $|y|$ and $|y - 1|$ are consecutive, therefore they are relatively prime. If the product of two relatively prime integers is a square, then each of them is a square. Since there is no example of two consecutive integers which are both squares, in $\mathbf{Z} \times \mathbf{Z}$ the given equation has only the two obvious solutions.

b) The geometric idea is to intersect the curve with a line through a rational point, for instance $(0, 0)$. Let $(x, y) \in \mathbf{Q} \times \mathbf{Q}$ be a solution with $x \neq 0$. Set $t = y/x$. Notice first that $t \neq \pm 1$ because $y = \pm x$ does not yield a solution when $x \neq 0$. Substitute tx to y in the equation, next divides by x which is not zero. One gets

$$x = \frac{t}{t^2-1} \quad \text{and} \quad y = \frac{t^2}{t^2-1}\cdot \tag{1}$$

For $t = 0$ these formulae (1) give the solution $(x, y) = (0, 0)$ but (1) does not produce the solution $(x, y) = (0, 1)$.

Conversely, if t is a rational number which is not 1 nor -1, then (x, y) given by (1) is solution of the equation. In conclusion (1) produces all rational solutions apart from $(0, 1)$.

Statement

3. Solve the equation $x^{15} = y^{21}$ in $\mathbf{Z} \times \mathbf{Z}$.

Solution

We first consider the equation $15a = 21b$ in rational integers $(a, b) \in \mathbf{Z} \times \mathbf{Z}$. This equation is equivalent to $5a = 7b$. Since 5 and 7 are relatively prime, the general solution is given by $(a, b) = (7c, 5c)$ with $c \in \mathbf{Z}$.

Now decompose x and y into prime factors. It follows that the general solution of the equation $x^{15} = y^{21}$ dans $\mathbf{Z} \times \mathbf{Z}$ is given by $(x, y) = (t^7, t^5)$ with t in $\mathbf{Z}$.

Remark. *Since the exponents* 15 *and* 21 *are odd,* x *et* y *have the same sign. For* $t > 0$ *one gets the positive solutions* (x, y)*, while* $t < 0$ *produce the negative solutions.*

Statement

4. Let $A = \mathbf{Z}[1/2]$ be the subring of $\mathbf{Q}$ spanned by $1/2$.

a) Is A a finitely generated $\mathbf{Z}$–module?

b) Which are the units of A?

Solution

a) Recall that a finitely generated $\mathbf{Z}$–module M is a $\mathbf{Z}$–module which if it is generated by a finite number of elements, which means that there is a finite subset $\{\gamma_1, \dots, \gamma_m\}$ of M such that

$$M = \mathbf{Z}\gamma_1 + \cdots + \mathbf{Z}\gamma_m.$$

Recall also that the right hand side denotes the set of linear combinations of the γ_j with coefficients in $\mathbf{Z}$:

$$\mathbf{Z}\gamma_1 + \cdots + \mathbf{Z}\gamma_m = \bigl\{a_1\gamma_1 + \cdots + a_m\gamma_m\ ;\ (a_1, \dots, a_m) \in \mathbf{Z}^m\bigr\}.$$

On the other hand the subring $A = \mathbf{Z}[1/2]$ of the rational number field $\mathbf{Q}$ generated by $1/2$ is the set of rational numbers $\ell/2^n$ with $\ell \in \mathbf{Z}$ and $n \in \mathbf{Z}$, $n \geq 0$.

Now if $\gamma_1, \dots, \gamma_m$ are elements in $A = \mathbf{Z}[1/2]$, then each of them can be written $\ell_j/2^{n_j}$. Let n be the largest of the n_j. Any linear combination of $\gamma_1, \dots, \gamma_m$ with integer coefficients is an integer r such that $2^n r$ is an integer. For instance $1/2^{n+1}$ is an element in A which is not in the $\mathbf{Z}$–module $\mathbf{Z}\gamma_1 + \cdots + \mathbf{Z}\gamma_m$. One deduces that A is not a finitely generated $\mathbf{Z}$–module.

The fact that the ring A is not a finitely generated $\mathbf{Z}$–module follows also from a theorem in the course together with the fact that $1/2$ is not integral over $\mathbf{Z}$.

b) An element $x = \ell/2^n$ in A is a unit in A if and only if there exists $x' = \ell'/2^{n'} \in A$ such that the product xx' is 1, which means $\ell\ell' = 2^{n+n'}$. Therefore ℓ and ℓ' are both powers of 2, up to a multiplicative coefficient -1. Conversely in the ring A any power of 2 with an exponent in $\mathbf{Z}$ is a unit: $2^j \cdot 2^{-j} = 1$ for any $j \in \mathbf{Z}$, and both factors 2^j, 2^{-j} are in A.

In conclusion the units in A are $\pm 2^j$, $j \in \mathbf{Z}$.

Statement

5. Which are the finitely generated sub–$\mathbf{Z}$–modules of the additive group $\mathbf{Q}$?

Solution

The answer is that they are the $\mathbf{Z}$–submodules of $\mathbf{Q}$ which are generated by a single element. One direction is clear: if γ is a rational number then $\mathbf{Z}\gamma$ is a finitely generated $\mathbf{Z}$–submodule of $\mathbf{Q}$. The problem is to prove the converse.

Let $\gamma_1, \dots, \gamma_m$ be rational numbers. If the γ_i are all 0 the $\mathbf{Z}$–module they generate is $\{0\}$ which is $\mathbf{Z}\gamma$ with $\gamma = 0$. Otherwise denote by q the least positive common denominator of the γ_i and set $p_i = q\gamma_i$. The numbers $q, p_1, \dots, p_m$ are positive integers with gcd 1. Denote by p the greatest common divisor of $p_1, \dots, p_m$, so that $\mathbf{Z}p = \mathbf{Z}p_1 + \cdots + \mathbf{Z}p_m$. Then p and q are relatively prime and the $\mathbf{Z}$–module $M = \mathbf{Z}\gamma_1 + \cdots + \mathbf{Z}\gamma_m$ is $\mathbf{Z}\gamma$ with $\gamma = p/q$.

Statement

6. Find the rational roots of the polynomial $X^7 - X^6 + X^5 - X^4 - X^3 + X^2 - X + 1$.

Solution

Recall that if p/q is a rational root with $\mathrm{pgcd}(p, q) = 1$ of a polynomial $a_0X^n + \cdots + a_n$ with coefficients in $\mathbf{Z}$ with $a_0a_n \neq 0$, then p divides a_n and q divides a_0. Here a_0 and a_n are both equal to 1, the only values to be tested are 1 and -1 and both are roots.

Statement

7. Let k be the number field $\mathbf{Q}(i, \sqrt{2})$.

a) What is the degree of k over $\mathbf{Q}$? Give a basis of k over $\mathbf{Q}$. Find $\gamma \in k$ such that $k = \mathbf{Q}(\gamma)$. Which are the conjugates of γ over $\mathbf{Q}$?

b) Show that k is a Galois extension of $\mathbf{Q}$. What is the Galois group? Which are the subfields of k?

Solution

a) The field k is the field generated by i and $\sqrt{2}$ over $\mathbf{Q}$, hence it contains $\sqrt{2}$ and i. Since the field $\mathbf{Q}(\sqrt{2})$ is contained in the field $\mathbf{R}$ of real numbers, it does not contain

i. Therefore k is an extension of degree 2 of $\mathbf{Q}(\sqrt{2})$ and therefore an extension of degree 4 of $\mathbf{Q}$.

A basis of $\mathbf{Q}(\sqrt{2})$ over $\mathbf{Q}$ (as a $\mathbf{Q}$–vector space) is $\{1, \sqrt{2}\}$, a basis of k over $\mathbf{Q}(\sqrt{2})$ is $\{1, i\}$, hence a basis of k over $\mathbf{Q}$ is obtained by taking the 4 products $\{1, \sqrt{2}, i, i\sqrt{2}\}$.

An example (among many!) of an element in k which is a generator of k over $\mathbf{Q}$ (here we consider field extensions: one is looking for a γ such that $k = \mathbf{Q}(\gamma)$) is $\gamma = i + \sqrt{2}$, since its 4 conjugates over $\mathbf{Q}$ are distinct: they are

$$i + \sqrt{2}, \quad i - \sqrt{2}, \quad -i + \sqrt{2}, \quad -i - \sqrt{2}.$$

b) The field k is the splitting field over $\mathbf{Q}$ of the polynomial $(X^2 - 2)(X^2 + 1)$ - it is also the splitting field over $\mathbf{Q}$ of the monic irreducible polynomial of γ which is, given our choice above for γ,

$$(X - i - \sqrt{2})(X - i + \sqrt{2})(X + i - \sqrt{2})(X + i + \sqrt{2}) = X^4 - 2X^2 + 9.$$

Hence k is a normal extension of $\mathbf{Q}$ (it is a splitting field) as well as a separable extension (the polynomial has no multiple roots - anyway we are here in zero characteristic).

The Galois group G of k over $\mathbf{Q}$ is the group of automorphisms of k. Such an automorphism is determined by its values at the points $\sqrt{2}$ and i. Its value at $\sqrt{2}$ is a conjugate of $\sqrt{2}$, hence is $\sqrt{2}$ or $-\sqrt{2}$. Similarly its value at i is a conjugate of i, hence is i or $-i$. This gives the four automorphisms we were looking for. Denote by σ the non–trivial automorphism of k which fixes i and by τ the automorphism which fixes $\sqrt{2}$ – then τ is the complex conjugation and $G = \{1, \sigma, \tau, \sigma\tau\}$ (here 1 is the unit element in the group G, namely the identity automorphism of k). Hence G is the non cyclic group of order 4, it is abelian of type $(2, 2)$ which means that it is isomorphic to $(\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z})$, and it has exactly 5 subgroups: two of them are the trivial subgroups $\{1\}$ and G, while the three others have order 2:

$$\{1, \sigma\}, \quad \{1, \tau\}, \quad \{1, \sigma\tau\}.$$

As a consequence of Galois theory k has exactly 5 subfields, two of them are the trivial ones k (the Galois group of k over k is $\{1\}$) and $\mathbf{Q}$ (the Galois group of k over $\mathbf{Q}$ is G), the three others are the subfields of k which are fixed by the three subgroups of order 2 respectively, they are the three quadratic subfields of k:

$$\mathbf{Q}(i), \quad \mathbf{Q}(\sqrt{2}), \quad \mathbf{Q}(i\sqrt{2}).$$

For instance let us check that $i\sqrt{2}$ is fixed by $\sigma\tau$: indeed $\sigma\tau(i) = \sigma(-i) = -i$ and $\sigma\tau(\sqrt{2}) = \sigma(\sqrt{2}) = -\sqrt{2}$. The Galois group of k over $\mathbf{Q}(i\sqrt{2})$ is $\{1, \sigma\tau\}$, as it should.

Statement

8. Let $\zeta \in \mathbf{C}$ satisfy $\zeta^5 = 1$ and $\zeta \neq 1$. Let $K = \mathbf{Q}(\zeta)$.
a) What is the monic irreducible polynomial of ζ over $\mathbf{Q}$? Which are the conjugates of ζ over $\mathbf{Q}$? What is the Galois group G of K over $\mathbf{Q}$? Which are the subgroups of G?
b) Show that K contains a unique subfield L of degree 2 over $\mathbf{Q}$. What is the ring of integers of L? What is its discriminant? What is the group of units?

Solution

a) The monic irreducible polynomial of ζ over $\mathbf{Q}$ is $X^4 + X^3 + X^2 + X + 1$. The conjugates of ζ over $\mathbf{Q}$ are the four roots of this polynomial, they are the four primitive fifth roots of unity in $\mathbf{C}$; if ζ is any of them, the others are $\zeta^2, \zeta^3, \zeta^4$. The Galois group of K over $\mathbf{Q}$ has four elements, which are the four automorphisms of K. Each of the four automorphisms is determined by the image of ζ, hence one can denote these automorphisms by $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ with $\sigma_j(\zeta) = \zeta^j$. The group G is cyclic, a generator is σ_2: indeed

$$\sigma_2^2(\zeta) = \sigma_2(\zeta^2) = \zeta^4, \quad \sigma_2^3(\zeta) = \sigma_2(\zeta^4) = \zeta^8 = \zeta^3,$$

hence $\sigma_2^2 = \sigma_4$, $\sigma_2^3 = \sigma_3$ and $G = \{1, \sigma_2, \sigma_2^2, \sigma_2^3\}$. Another generator is σ_2^3 (this is due to the fact that the exponent 3 is prime to the order of the group 4).
b) The group G is cyclic of order 4; since 4 has three divisors (1, 2, 4) it follows that G has 3 subgroups, two of them are the trivial subgroups $\{1\}$ and G, the third one is the unique subgroup H of G of order 2, it is generated by the unique element of order 2, namely σ_2^2. Since $\sigma_2^2(\zeta) = \zeta^4$ is the complex conjugate of ζ (recall $\zeta^5 = 1$, $|\zeta|^2 = \zeta\bar{\zeta} = 1$ hence $\zeta^4 = \zeta^{-1} = \bar{\zeta}$), the subfield L of K which is fixed by H is the intersection of K and $\mathbf{R}$.

Set $\alpha = \zeta + \bar{\zeta}$, so that $\alpha \in K \cap \mathbf{R}$. Since

$$\alpha^2 = (\zeta + \bar{\zeta})^2 = \zeta^2 + \bar{\zeta}^2 + 2 \quad \text{and} \quad 1 + \zeta + \zeta^2 + \bar{\zeta}^2 + \bar{\zeta} = 0,$$

we have $\alpha^2 + \alpha - 1 = 0$. The real part of ζ is positive, hence α is the golden number $(1 + \sqrt{5})/2$. The field L is the field $\mathbf{Q}(\sqrt{5})$, its ring of integers is $\mathbf{Z} + \mathbf{Z}\alpha$, its discriminant is 5, the group of units is $\{\pm\alpha^m \; ; \; m \in \mathbf{Z}\}$.