Kris Harper
MATH 24200
May 24, 2010

Homework 6

Problem 1. *Find the minimal polynomial for* $\sqrt{3}+\sqrt{7}$.

Proof. Note $(\sqrt{3}+\sqrt{7})^4 - 20(\sqrt{3}+\sqrt{7})^2 + 16 = 0$ so $\sqrt{3}+\sqrt{7}$ satisfies $x^4 - 20x^2 + 16$. Note that putting in ± 1, ± 2, ± 4, ± 8 and ± 16 gives -3, 37, -8, 72, 192, 352, 3952, 4272, 65232 and 65872 respectively so by the rational root theorem we know this polynomial has no linear factors. Suppose $x^4 - 20x + 16 = (x^2+ax+b)(x^2+cx+d) = x^4 + (a+c)x^3 + (b+ac+d)x^2 + (ad+bc)x + bd$. Then we have $a+c=0$, $b+ac+d=-20$, $ad+bc=0$ and $bd=16$. Note that $a=-c$ so $a(d-b)=0$ and either $a=0$ or $b-d=0$. First suppose $a=0$ so that $b+d=-20$ and $bd=16$. Then $d=16/b$ and $b^2+20b+16=0$. Since $20^2-64=336$ is not a square, we see that b must be irrational. This is a contradiction, so we must have $b-d=0$ or $b=d$. Then since $bd=16$, $b=d=\pm 4$, but then clearly $b+d\neq -20$, another contradiction. This shows $x^4-20x+16$ can't be factored into two quadratics and thus must be irrational. Since $\sqrt{3}+\sqrt{7}$ satisfies this irreducible monic polynomial, it must be the minimal polynomial. □

Problem 2. *Compute the discriminant of* $\mathbb{Q}(\sqrt{2}+\sqrt{5})$.

Proof. Note that $(\sqrt{5}+\sqrt{2})^4 - 14(\sqrt{5}+\sqrt{2})^2 + 9 = 0$ so $\sqrt{2}+\sqrt{5}$ satisfies x^4-14x^2+9. Furthermore, this polynomial is irreducible by a similar process to that used in Problem 1. It's easy to check that all the roots are $\pm\sqrt{2}\pm\sqrt{5}$ so we have automorphisms $\sigma_2 : \sqrt{2}\mapsto -\sqrt{2}$, $\sigma_3 : \sqrt{5}\mapsto -\sqrt{5}$, $\sigma_4 = \sigma_2\sigma_3$ and the identity σ_1. Let $\alpha_1 = 1$, $\alpha_2 = \sqrt{2}+\sqrt{5}$, $\alpha_3 = (\sqrt{2}+\sqrt{5})^2$ and $\alpha_4 = (\sqrt{2}+\sqrt{5})^3$ so that α_i form a basis. Then we can directly compute $\delta(\mathbb{Q}(\sqrt{2}+\sqrt{5}) = \Delta(\alpha_1,\alpha_2,\alpha_3,\alpha_4) = \det(\sigma_i(\alpha_j))^2 = 1600$. □

Problem 3. *Describe the units in* $\mathbb{Q}(\sqrt{5})$.

Proof. Let $a+b\sqrt{5}\in\mathbb{Q}(\sqrt{5})$ so that $a,b\in\mathbb{Q}$ and $a+b\sqrt{5}\neq 0$. Then note $(a+b\sqrt{5})(c+d\sqrt{5}) = (ac+5bd)+(ad+bc)\sqrt{5}$. Set $ac+5bd=1$ an $ad+bc=0$ so that $c=-ad/b$. Then $1=a(-ad/b)+5bd = -a^2d/b+5bd = d(-a^2/b+5b)$ and $d=(-a^2/b+5b)^{-1} = b/(5b^2-a^2)$. This also gives $c=-a/(5b^2-a^2)$ so that $(a+b\sqrt{5})^{-1} = 1/(5b^2-a^2)(-a+b\sqrt{5})$. □

Problem 4. *If* D *is the ring of integers in an algebraic number field and* $\mathfrak{B}$ *is a prime ideal such that* $\mathfrak{B}=(\alpha)$ *then show that* α *is irreducible.*

Proof. Suppose $\alpha = ab$. Then $ab\in(\alpha)$ so at least one of a or b is in (α). Without loss of generality suppose $a\in(\alpha)$. Then $a=\alpha c$ for some c. But then $\alpha = ab = \alpha cb$ so $cb=1$ forcing b to be a unit. Therefore α is irreducible. □

Problem 5. *Show that the class number of* $\mathbb{Q}(\sqrt{-5})$ *is greater than one.*

Proof. Note that $21 = (1+2\sqrt{-5})(1-2\sqrt{-5})$. Since every ideal can be written uniquely as a product of prime ideals, we see that $(1+2\sqrt{-5})$ and $(1-2\sqrt{-5})$ have different prime factorizations, thus they must be in different ideal equivalence classes. This shows that there are at least two classes. □

Problem 6. *Let* $\alpha_1,\ldots,\alpha_n\in D$, *the ring of integers in a number field* F, $\Delta(\alpha_1,\ldots,\alpha_n)\neq 0$. *Show that if* $\Delta(\alpha_1,\ldots,\alpha_n)$ *is a product of distinct primes (i.e.,* Δ *is square free) then* $\alpha_1,\ldots,\alpha_n$ *is an integral basis. Conclude that if* d *is square free* $d\equiv 1 \pmod 4$ *then* $(1+\sqrt{d})/2$, 1 *form an integral basis for the ring of integers in* $\mathbb{Q}(\sqrt{d})$.

Proof. Note that since $\Delta(\alpha_1\ldots,\alpha_n)\neq 0$ we know these form a basis for $F/\mathbb{Q}$. Suppose $\Delta(\alpha_1,\ldots,\alpha_n)$ is not squarefree. Then we can factor out some square term in the discriminant and write this as the square of the determinant of some matrix (since the determinant map is surjective). But then we can view this matrix as a change of basis matrix so that $\Delta(\alpha_1,\ldots,\alpha_n) = \det(a_{ij})^2\Delta(\beta_1,\ldots,\beta_n)$ for some other basis $\beta_1,\ldots\beta_n$. Thus

$\Delta(\alpha_1,\ldots,\alpha_n) < \Delta(\beta_1,\ldots,\beta_n)$ so that if $\Delta(\alpha_1,\ldots,\alpha_n)$ is squarefree then $|\Delta(\alpha_1,\ldots,\alpha_n)|$ is minimal. But then this means $\alpha_1,\ldots,\alpha_n$ form an integral basis for D. In particular, if $alpha_1 = 1$ and $\alpha_2 = (1+\sqrt{d})/2$ then note that

$$(\mathrm{tr}(\alpha_i\alpha_j)) = \begin{pmatrix} 2 & -1 \\ -1 & (1+d)/2 \end{pmatrix}$$

so we have $\Delta(\alpha_1,\alpha_2) = \det(\mathrm{tr}(\alpha_i\alpha_i)) = d$. Since d is assumed to be squarefree we must have 1, $(1+\sqrt{d})/2$ is an integral basis for D. □

Problem 7. *Show that $(3, 1+\sqrt{-5})$ is a proper ideal in $\mathbb{Z}[\sqrt{-5}]$. Is it prime?*

Proof. Suppose $1 = 3a + (1+\sqrt{-5})b$ for some integers a and b. Then $1 = (3a+b) + b\sqrt{-5}$ so we must have $b = 0$. But then $3a = 1$ and $a = 1/3$, a contradiction. Thus $1 \notin (3, 1+\sqrt{-5})$ and this ideal must be proper. Now consider the quotient ideal $R = \mathbb{Z}[\sqrt{-5}]/(3, 1+\sqrt{-5})$. Let $(a+b\sqrt{-5}), (c+d\sqrt{-5}) \in R$ such that $0 = (a+b\sqrt{-5})(c+d\sqrt{-5}) = (ac-5bd) + (ad+bc)\sqrt{-5}$. Then we can write $ac - 5bd = 3e + ad - bc$ for some integer e so that $(a+b\sqrt{-5})(c+d\sqrt{-5}) = 3e + (ad-bc)(1+\sqrt{-5})$. Note then that $a(c-d) = 5bd + 3e - bc = b(5d-c) + 3e$. If we assume $3 \nmid (c-d)$ (so that $c+d\sqrt{-5} \neq 0$ in R), then we get $a = 3f + b$ for some integer f. But then $a + b\sqrt{-5} = 3f + b(1+\sqrt{-5}) = 0$ in R. This shows that R is an integral domain so $(3, 1+\sqrt{-5})$ must be a prime ideal. □

Problem 8. *Let F be an algebraic number field, D its ring of integers. Suppose the class number of F is 2. Show that if π is an irreducible such that (π) is not prime then $(\pi) = \mathfrak{B}_1\mathfrak{B}_2$ where $\mathfrak{B}_1$, $\mathfrak{B}_2$ are (not necessarily distinct) prime ideals.*

Proof. Since (π) is not prime we know there exist ideals $\mathfrak{B}_1$ and $\mathfrak{B}_2$ such that $(\pi) = \mathfrak{B}_1\mathfrak{B}_2$ and neither ideal is contained in (π). Suppose P_1 and P_2 are prime ideals such that $P_1 \sim P_2$. Then there exist a and b such that $(a)P_1 = (b)P_2$ and $(a/b)P_1 = P_2$. But P_2 is prime so by unique factorization we must have $(a/b) = D$ and $P_1 = P_2$. Thus any two distinct prime ideals belong to distinct equivalence classes. Since the class number is 2 we see that $\mathfrak{B}_1$ and $\mathfrak{B}_2$ cannot have more than 1 prime factor because then we would have three distinct prime ideals leading to more than 2 equivalence classes. Thus $\mathfrak{B}_1$ and $\mathfrak{B}_2$ each have at most one prime factor so they must be prime. □