Problem Set 1.

1. Find a monic polynomial with integer coefficients which has $\sqrt{7}+\sqrt{13}$ as a root.
2. Show that given integers $r_1 \geq 0, r_2 \geq 0, r_1 + r_2 \geq 1$ there exists a number field K such that $K \otimes_{\mathbf{Q}} \mathbf{R} = \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ as an algebra.
3. Let D be a square free integer (not equal to 0 or 1). Find the maximal order of the number field $\mathbf{Q}(\sqrt{D})$. Show that any order in the number field $\mathbf{Q}(\sqrt{D})$ is determined by its index in the maximal order and explicitly describe all orders is this field. (An order $\mathcal{O}$ in a number field K is a subring which is finitely generated as an abelian group and contains a basis for the rational vector space K)
4. Let $\mathcal{O} = \mathbf{Z}[\omega]$ be an order in a complex quadratic field
   a) Show that the order $\mathcal{O}$ above is Euclidean with respect to the function σ given by the square of the distance in the complex plane from the origin when $\sigma(\omega) < 3$. Hint: note that given nonzero $\alpha \in \mathcal{O}$ any element of the order $\mathcal{O}$ is in a rotation of a parallelogram with one side parallel to the x-axis of length $|\alpha|$ and the other side of length $|\alpha\omega|$. The barycenter of this parallelogram is the farthest point from elements of the lattice. Show that the distance from any $\beta \in \mathcal{O}$ to $\alpha\mathcal{O}$ is at most $|\alpha|\sqrt{(1+|\omega|^2)/4}$.
   b) Show that $\mathbf{Z}[\sqrt{-1}], \mathbf{Z}[\sqrt{-2}]$ and $\mathbf{Z}[(1+\sqrt{-3})/2]$ are Euclidean domains.
   c) Show that $\mathbf{Z}[\sqrt{-3}]$ and $\mathbf{Z}[\sqrt{-5}]$ are not Euclidean domains.
   d) Explain why the proof that the orders in b) are Euclidean does not work for the orders in c).
5. The argument of the complex number $a + bi$ is $\arctan(b/a)$. Show that the factorization of the Gaussian integer $3 + i$ into irreducibles leads by taking the argument of the complex numbers involved to the pleasant formula $\arctan(1/1) = \arctan(1/2) + \arctan(1/3)$. Prove by a similar method using factorization in the field $\mathbf{Z}[i]$ that the following formulas of Machin and Gauss respectively hold:

$$\arctan(1) = 4\arctan(1/5) - \arctan(1/239)$$

$$\arctan(1) = 12\arctan(1/18) + 8\arctan(1/57) - 5\arctan(1/239)$$

6. Next to each polynomial is printed the degrees of the irreducible factors mod p, where d,m means an irreducible factor of degree d appears to power m (and a semicolon separates the information for different irreducible factors). Also given is the count C of the number of primes from the 9592 primes less than 10^5 for which the polynomial

factors completely into linear factors. Using the given information together with construction of Frobenius elements and cycle structure, show that each polynomial is irreducible and predict as much as you can about the Galois group of the splitting field over the rational field, for example the order and any other information you can. You may wish to use that the group is a subgroup of a particular symmetric group, that certain Frobenius elements are described via cycle structure as permutations so that the order of the Frobenius element is evident.

	C	2	3	5	7	11	13	17	19
x^3-2	1559	[1, 3]	[1, 3]	[1, 1; 2, 1]	[3, 1]	[1, 1; 2, 1]	[3, 1]	[1, 1; 2, 1]	[3, 1]
x^3+x^2-2x-1	3189	[3, 1]	[3, 1]	[3, 1]	[1, 3]	[3, 1]	[1, 1; 1, 1; 1, 1]	[3, 1]	[3, 1]
x^4-x^2-2	2384	[1, 2; 1, 2]	[2, 2]	[1, 1; 1, 1; 2, 1]	[1, 1; 1, 1; 2, 1]	[2, 1; 2, 1]	[1, 1; 1, 1; 2, 1]	[1, 1; 1, 1; 1, 1; 1, 1]	[2, 1; 2, 1]
$x^4+x^3+x^2+x+1$	2387	[4, 1]	[4, 1]	[1, 4]	[4, 1]	[1, 1; 1, 1; 1, 1; 1, 1]	[4, 1]	[4, 1]	[2, 1; 2, 1]
x^7-7x+3	50	[7, 1]	[1, 1; 1, 3; 1, 3]	[7, 1]	[1, 7]	[7, 1]	[1, 1; 2, 1; 4, 1]	[1, 1; 3, 1; 3, 1]	[1, 1; 3, 1; 3,
$x^6+2x^5+3x^4+4x^3+5x^2+6x+7$	76	[1, 6]	[6, 1]	[3, 1; 3, 1]	[1, 1; 1, 5]	[6, 1]	[1, 1; 5, 1]	[1, 1; 5, 1]	[1, 1; 1, 1; 4,
x^4-4x^2+10	1196	[1, 4]	[2, 2]	[1, 1; 1, 1; 1, 2]	[1, 1; 1, 1; 2, 1]	[1, 1; 1, 1; 2, 1]	[2, 1; 2, 1]	[4, 1]	[4, 1]
x^4-2	1182	[1, 4]	[2, 1; 2, 1]	[4, 1]	[1, 1; 1, 1; 2, 1]	[2, 1; 2, 1]	[4, 1]	[2, 1; 2, 1]	[2, 1; 2, 1]