# MAT 314: HOMEWORK 7

DUE TH, MARCH 30, 2023

Throughout this problem set, $\mathbb{F}$ is a field.

**1.** Find degree and minimal polynomial over $\mathbb{Q}$ of the following complex numbers:
   (a) $\sqrt{-3}+\sqrt{2}$
   (b) $\sqrt{1+\sqrt{2}}$

**2.** For each of the following polynomials, describe its splitting field over $\mathbb{Q}$.
   (a) $x^4+1$
   (b) $x^3-5$
   (c) $x^3+3x+1$ (hint: how many roots does it have in $\mathbb{R}$?)
   (d) $x^4+x^2+1$

**3.** A number $z \in \mathbb{C}$ is called *primitive* $n$th root of unity if $z^n=1$, but for all $1 \le k < n$, we have $z^k \neq 1$.
   (a) Show that if $z$ is a primitive $n$th root of unity, then all other primitive $n$th roots of unity in $\mathbb{C}$ are $z^k$, where $k$ is relatively prime with $n$. In particular, the number of such primitive roots of unity is $\varphi(n)$, where $\varphi(n)$ is Euler's function.
   (b) Define the *cyclotomic polynomial*

$$\Phi_n(x) = \prod (x-z_i) \in \mathbb{C}[x]$$

   where the product is taken over all primitive $n$th roots of unity in $\mathbb{C}$. In particular,

$$\deg \Phi_n = \varphi(n).$$

   Prove that then

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

   where the product is taken over divisors $d$ of $n$ (including 1 and $n$).
   (c) Prove that $\Phi_n(x)$ has integer coefficients [Hint: $\Phi_n = (x^n-1)/\prod \Phi_d(x)$, where the product is over all divisors of $n$ excluding $n$ itself.]
   (d) Compute the following cyclotomic polynomials:
      (i) $\Phi_p(x)$, where $p$ is prime
      (ii) $\Phi_6(x)$
      (iii) $\Phi_4(x)$
      (iv) $\Phi_{12}(x)$.

The cyclotomic polynomials play an important role in the study of field extensions. It is known that for any $n$, $\Phi_n(x)$ is irreducible over $\mathbb{Q}$.

**4.** Let now $K$ be an arbitrary field and let $\Phi_n(x)$ be cyclotomic polynomials defined in the previous problem. Since they have integer coefficients, they can also be considered as elements in $K[x]$; moreover, the formula

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

also holds over any field.

As before, we call a number $z \in K$ *primitive* $n$th root of unity if $z^n = 1$, but for all $1 \leq k < n$, we have $z^k \neq 1$.

(a) Prove that if $z \in K$ a primitive $n$th root of unity in $K$, then $z$ is a root of $\Phi_n(x)$. Deduce from this that in any field, the number of primitive $n$-th roots of unity is at most $\varphi(n)$.

(b) Use the previous part and the formula $\sum_{d|n} \varphi(d) = n$ to prove that if $G \subset K^\times$ is a finite subgroup in $K^\times = K - \{0\}$ (with respect to multiplication), then $G$ contains at least one primitive $n$-th root of unity. Deduce from this that $G$ is cyclic.

**5.** Let $z = e^{2\pi i/5} \in \mathbb{C}$, and let $t = (z + z^{-1})/2 = \cos(2\pi/5)$.

(a) Show that we have a chain of extensions

$$\mathbb{Q} \subset \mathbb{Q}(t) \subset \mathbb{Q}(z)$$

and $[\mathbb{Q}(z) : \mathbb{Q}(t)] = [\mathbb{Q}(t) : \mathbb{Q}] = 2$.

(b) Find the minimal polynomials of $t, z$.

(c) Write a formula for $z$ which only uses rational numbers, arithmetic operations, and square roots.