B3.1 Galois Theory Sheet 3 (MT 2018)

In these problems K denotes an arbitrary field and $K[x]$ denotes the ring of polynomials in one variable x over K. If p is a prime number, then $\mathbb{F}_p$ denotes the field of integers modulo p.

1. Let $\Phi_m(x) \in \mathbb{C}[x]$ be the m-th cyclotomic polynomial, the monic polynomial whose roots are the primitive mth roots of 1 in $\mathbb{C}$. Show that
   (a) $\Phi_1(x) = x - 1$; $\Phi_2(x) = x + 1$; $\Phi_3(x) = x^2 + x + 1$; $\Phi_4(x) = x^2 + 1$.
   (b) $\prod_{d|m} \Phi_d(x) = x^m - 1$.
   (c) $\Phi_m(x) \in \mathbb{Z}[x]$. [Hint: prove first that $\Phi_m(x) \in \mathbb{Q}[x]$ by induction on m).
   (d) If p is prime then $\Phi_p(x) = 1 + x + x^2 + \cdots + x^{p-1}$ and $\Phi_{p^n}(x) = \Phi_p(x^{p^{n-1}})$.
   (e) $\deg \Phi_{nm} = \deg \Phi_m \deg \Phi_n$ if (m, n) are relatively prime.

2. Let n be a positive integer and $f = x^{p^n} - x \in \mathbb{F}_p[x]$. Let M be the splitting field of f over $\mathbb{F}_p$. Show that M consists exactly of the set of roots of f. Show that $[M : \mathbb{F}_p] = n$. Explain why this fact also shows the existence of an irreducible polynomial of degree n in $\mathbb{F}_p[x]$.

3. (a) Prove that $\Phi_{12}(x) = x^4 - x^2 + 1$, and that it is irreducible over $\mathbb{Q}$. Factorise it into irreducibles over $\mathbb{F}_p$ when $p = 2, 3, 5, 13$.
   (b) If p is any prime with $p > 3$ show that $p^2 - 1$ is divisible by 12, and deduce that Φ_{12} is reducible over $\mathbb{F}_p$ for every prime p.

4. For this exercise recall the definition of a group action on a set. Let $f \in K[x]$ be a separable degree n polynomial, let M be its splitting field and $G = \Gamma(M : K)$ be the Galois group of M. Let $A = \{\alpha_1, \dots \alpha_n\} \subseteq M$ be the set of roots of f. Let $S(A)$ be the set of permutations of the roots of f.
   (a) Show that G acts faithfully on A (this is equivalent to showing that there is an injective group homomorphism between G and $S(A)$).
   (b) Show that if f is irreducible, then G acts transitively on A (this is equivalent to show that for any $\alpha_i, \alpha_j \in A$ there exists $\sigma \in G$ such that $\sigma(\alpha_i) = \alpha_j$).

5. Find the Galois groups of the following polynomials and for each subgroup identify the corresponding subfield of the splitting field:
   (a) $x^2 + 1$ over $\mathbb{R}$;
   (b) $x^3 - 1$ over $\mathbb{Q}$;
   (c) $x^3 - 5$ over $\mathbb{Q}$;
   (d) $x^6 - 3x^3 + 2$ over $\mathbb{Q}$;

(e) $x^5 - 1$ over $\mathbb{Q}$;

(f) $x^6 + x^3 + 1$ over $\mathbb{Q}$.

(g) $x^{p^n} - x - t$ over $\mathbb{F}_{p^n}(t)$ (you can assume that this polynomial is irreducible over $\mathbb{F}_{p^n}(t)$)

6. Prove that $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ is Galois over $\mathbb{Q}$, and find its Galois group.