Student seminar solutions Week 1

1. *Let G be a finite group of automorphisms of a ring A and let*

$$A^G = \{a \in A | \sigma(a) = a \text{ for all } \sigma \in G\} \tag{1}$$

be the ring of invariants.

(a) *Show that A is integral over A^G.*

Given $a \in A$, consider the polynomial:

$$f(X) = \prod_{\sigma \in G} (X - \sigma(a)) \tag{2}$$

(here one use the fact that G is finite): it is a monic polynomial with root a. As $\sigma(f(X)) = f(\sigma(X))$ for all $\sigma \in G$, $f \in A^G[X]$, hence by definition a is integral over A^G, and furthermore A is integral over A^G.

(b) *Let $\mathfrak{p} \subset A^G$ be a prime ideal and P the set of prime ideals $\mathfrak{q} \subset A$ such that $\mathfrak{q} \cap A^G = \mathfrak{p}$. Show that G acts transitively on P.*

Consider $\mathfrak{q}_1, \mathfrak{q}_2 \in P$, we will show that $\mathfrak{q}_2 = \sigma(\mathfrak{q}_1)$ for some $\sigma \in G$. Consider $a \in \mathfrak{q}_2$, then

$$b := \prod_{\sigma \in G} \sigma(a) = a \cdot \prod_{\sigma \neq 1} \sigma(a) \in \mathfrak{q}_2 \tag{3}$$

but b is by construction G-invariant, i.e.:

$$b \in \mathfrak{q}_2 \cap A^G = \mathfrak{p} = \mathfrak{q}_2 \cap A^G \subset \mathfrak{q}_1 \tag{4}$$

but, as $\mathfrak{q}_1$ is prime, there is some $\sigma \in G$ such that $\sigma^{-1}(a) \in \mathfrak{q}_1$, i.e. $a \in \sigma(\mathfrak{q}_1)$. Such a σ exists for any $a \in \mathfrak{q}_2$, hence we have:

$$\mathfrak{q}_2 \subset \bigcup_{\sigma \in G} \sigma(\mathfrak{q}_1) \tag{5}$$

but, if an ideal is contained in a finite union of prime ideals, then it is contained in one of those prime ideal (this is the prime avoidance lemma, which can be proven by induction over n). Then there is

some $\sigma \in G$ such that $\mathfrak{q}_2 \subset \sigma(\mathfrak{q}_1)$. Similarly, there is some $\sigma' \in G$ such that $\mathfrak{q}_1 \subset \sigma'(\mathfrak{q}_2)$, such that:

$$\mathfrak{q}_2 \subset \sigma(\mathfrak{q}_1) \subset \sigma'\sigma(\mathfrak{q}_2) \subset \cdots \subset (\sigma'\sigma)^n(\mathfrak{q}_2) \subset \tag{6}$$

but, as G is finite, $\sigma'\sigma$ has finite order, hence this sequence of inclusion is a sequence of equality, and then $\mathfrak{q}_2 = \sigma(\mathfrak{q}_1)$ as claimed.

2. *Show that the ideal $J = (2, 1+\sqrt{-5})$ is not principal in $\mathbb{Z}[\sqrt{-5}]$. In particular the ideal class group of $\mathbb{Q}[\sqrt{-5}]$ is not trivial.*

We compute the norm of the given generators of J:

$$\begin{aligned} N(a+b\sqrt{-5}) &:= (a+b\sqrt{-5})(a-b\sqrt{-5}) = a^2+5b^2 \\ N(2) &= 4 \\ N(1+\sqrt{-5}) &= 6 \end{aligned} \tag{7}$$

Supposing that $J = (\alpha)$ for $\alpha \in \mathbb{Z}[\sqrt{-5}]$, we will raise a contradiction. Then α would divide 2 and $1+\sqrt{-5}$, hence, by multiplicativity of the norm, α would divide 4 and 6, i.e. $N(\alpha) = 2$ or $N(\alpha) = 1$. There is no element of norm 2, hence $N(\alpha) = 1$, $\alpha = \pm 1$ and $J = \mathbb{Z}[\sqrt{-5}]$. But, reducing modulo 2, one obtains the ideal $\hat{J} \subset \mathbb{F}_2[\sqrt{-5}] = \mathbb{F}_2$ (i.e., 1 is a square root of -5 in $\mathbb{F}_2$). But $\hat{2} = 0 \in \mathbb{F}_2$, and $1+\hat{\sqrt{-5}} = 1+1 = 0 \in \mathbb{F}_2$, hence $\hat{J} = \{0\} \subsetneq \mathbb{F}_2$, hence $J \subsetneq \mathbb{Z}[\sqrt{-5}]$, giving a contradiction. Then J is not principal, i.e. there is a non principal ideal in $\mathbb{Z}[\sqrt{-5}]$, which is the ring of integer in $\mathbb{Q}[\sqrt{-5}]$ (as $-5 \equiv 3 \pmod 4$), hence by definition the ideal class group of $\mathbb{Q}[\sqrt{-5}]$ is not trivial.

3. *Give examples of extensions of number fields K/F and prime ideal $\mathfrak{p} \subset \mathcal{O}_F$ that are unramified, ramified, inert and completely split in K/F.*

Consider the extension $\mathbb{Q}[\sqrt{3}]/\mathbb{Q}$, we have:

- $(3) = (\sqrt{-3})^2$, i.e. the prime ideal (3) of $\mathbb{Z}$ is ramified in the extension $\mathbb{Q}[\sqrt{3}]/\mathbb{Q}$.
- $3 \equiv 4^2 \pmod{13}$, in particular $(13) = (4-\sqrt{3})(4+\sqrt{3})$, hence the prime ideal (3) of $\mathbb{Z}$ is completely split in $\mathbb{Q}[\sqrt{3}]/\mathbb{Q}$. In particular, it is also unramified.
- 3 is not a prime modulo 5, hence the polynomial X^2-3 is irreducible modulo 5, i.e. (5) is still prime in $\mathbb{Z}[\sqrt{3}]$, and then 5 is inert in $\mathbb{Q}[\sqrt{3}]/\mathbb{Q}$. In particular, it is also unramified.

4. *Show that the cyclotomic polynomial $\Phi_n \in \mathbb{Z}[X]$ factors into distinct linear factors modulo a prime p if and only if $p \equiv 1 \pmod{n}$*

First, we use the recursive definition of the cyclotomic polynomial:

$$X^n - 1 = \prod_{d|n} \Phi_d(X) \tag{8}$$

as this definition works over any ring: in particular, the reduction $(\Phi_n)_p \in \mathbb{F}_p[X]$ of the cyclotomic polynomial still verify this definition. For any d, $(\Phi_d)_p(X)|X^d - 1$, i.e. a root of $(\Phi_d)_p(X)$ is a d-th root of unity. We prove by induction that the roots of $(\Phi_n)_p(X)$ are exactly the n-th root of unity. For $n = 1$, this is trivial. Assume that we have proven it for any $d|n$ such that d is not n: then, in the decomposition:

$$X^n - 1 = (\Phi_n)_p(X) \times \prod_{d|n, d\neq n} (\Phi_d)_p(X) \tag{9}$$

we have that the roots of the second members are exactly the primitive d-th roots of unity for any d dividing strictly n, hence by definition the roots of $(\Phi_n)_p(X)$ are exactly the primitive n-th roots of unity in $\mathbb{F}_p$.

By definition, the primitive n-th roots of unity in $\mathbb{F}_p$ are the elements of order exactly n in the multiplicative group $\mathbb{F}_p^\times$. Then $(\Phi_n)_p(X)$ is a product of linear factors in $\mathbb{F}_p[X]$, i.e. $\Phi_n(X)$ completely splits modulo p, iff $\mathbb{F}_p^\times$ contains $\varphi(n)$ elements of order n (where we denote by $\varphi(n)$ the numbers of $1 \leq m \leq n-1$ which are prime to n). But $\mathbb{F}_p^\times$ is a cyclic group of order $p-1$, hence it contains a cyclic group of order n (which contains then $\varphi(n)$ elements of order n) iff $n|p-1$, i.e. $n \equiv 1$ (mod p). Then $\mathbb{F}_p$ has $\varphi(n)$ distinct primitive n-th roots of unity iff $n \equiv 1$ (mod p).