Galois Representations

Solved exercises - Part 2

Aalto University

We cover the problems from Lecture 2 of Fernando Gouvêa's notes "Deformations of Galois Representations" which were solved (or partially solved) in class. We leave some simple details for you.

Problem 2.1.

Show that the p-Frattini quotient of Π exists and that it is the image of a surjective continuous homomorphism from $\Pi^{(p)}$.

Hints.

Consider $\Pi/p\Pi$ and use Zorn's lemma.

Problem 2.3.

Prove that objects of $\mathcal{C}$ are pro-objects of $\mathcal{C}^0$. Specifically, prove that if R is a complete noetherian local ring with maximal ideal $\mathfrak{m}$, then for every n the quotient $R/\mathfrak{m}^n$ is an object in $\mathcal{C}^0$, and R is the inverse limit of the $R/\mathfrak{m}^n$.

Solution.

Let R be an object in $\mathcal{C}$, that is, a complete noetherian local ring. Let $\mathfrak{m}$ be the maximal ideal of R. Recall that the objects in $\mathcal{C}^0$ are artinian local rings, where artinian means that all descending chains of ideals stabilizes. We aim at showing that R is the inverse limit of $R/\mathfrak{m}^n$, where for every n, $R/\mathfrak{m}^n$ is an artinian local ring.

The fact that R is complete implies directly that it is the inverse limit of $R/\mathfrak{m}^n$. Hence, it remains to show that, for every n, $R/\mathfrak{m}^n$ is an artinian local ring. It is clearly local with maximal ideal $\mathfrak{m}/\mathfrak{m}^n$. To see that it is artinian, we note that the only descending chains of ideals in $R/\mathfrak{m}^n$ are of the form

$$\mathfrak{m}^k/\mathfrak{m}^n \supseteq \mathfrak{m}^{k+1}/\mathfrak{m}^n \supseteq \mathfrak{m}^{k+2}/\mathfrak{m}^n \supseteq \dots,$$

where $k < n$. But

$$\mathfrak{m}^n/\mathfrak{m}^n = \{0\}$$

and so the chain stabilizes.

Problem 2.6.

Show that any coefficient ring R in $\mathcal{C}$ carries a canonical $W(k)$ algebra structure. (That is, show that every such R has a unique coefficient ring homomorphism $W(k) \to R$).

Solution.

We solved this exercise only for the particular case $k = \mathbb{F}_p$ for some prime p. In that case $W(k) = \mathbb{Z}_p$. So we will show that every coefficient ring R over $k = \mathbb{F}_p$ has a unique coefficient ring homomorphism $\mathbb{Z}_p \to R$.

By definition of coefficient ring over $k = \mathbb{F}_p$, we have that

$$R/\mathfrak{m} \cong \mathbb{F}_p$$

and

$$R = \varprojlim_n R/\mathfrak{m}^n.$$

Consider the unique ring homomorphism $\iota : \mathbb{Z} \to R$ (the one taking $1 \in \mathbb{Z}$ to the unity of R). Let (n) be the ideal of $\mathbb{Z}$ satisfying $\iota(n) = \mathfrak{m}$. Then ι induces a ring homomorphism $\mathbb{Z}/(n) \to R/\mathfrak{m} \cong \mathbb{F}_p$. For this to be a ring homomorphism, we need to have $(n) = (p)$, and so $\iota(p) = \mathfrak{m}$.

In that case, for every $n \geq 1$, ι induces a unique ring homomorphism

$$\mathbb{Z}/p^n\mathbb{Z} \to R/\mathfrak{m}^n.$$

Moreover, this system of homomorphisms induces a unique ring homomorphism

$$\varprojlim_n \mathbb{Z}/p^n\mathbb{Z} \to \varprojlim_n R/\mathfrak{m}^n,$$

where both the inverse systems defining the inverse limits are given by the reduction homomorphisms $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^k\mathbb{Z}$ and $R/\mathfrak{m}^n \to R/\mathfrak{m}^k$, whenever $k|n$. Note that the domain of the last homomorphism coincides with $\mathbb{Z}_p$ and the codomain coincides with R. Note furthermore that by definition of ι the map takes (p) to a subset of $\mathfrak{m}$ (check this), and so it is a coefficient ring homomorphism. We have thus obtained a unique coefficient ring homomorphism

$$\mathbb{Z}_p \to R.$$

Problem 2.7.

Show that in fact every coefficient ring is the quotient of a power series ring in several variables with coefficients in $W(k)$.

Sketch of solution.

This result is called the Cohen structure theorem. As in Problem 2.6., we consider only the particular case $k = \mathbb{F}_p$ and $W(k) = \mathbb{Z}_p$. So we need to show that

$$R \cong \mathbb{Z}_p[[x_1, \ldots, x_n]]/I$$

for some variables $x_1, \ldots, x_n$ and an ideal $I \subseteq R$.

Since R is a coefficient ring, it is noetherian. In particular, its maximal ideal $\mathfrak{m}$ is finitely generated, say $\mathfrak{m} = (y_1, \ldots, y_n)$. From Problem 2.6., there exists a unique coefficient ring homomorphism

$$\iota : \mathbb{Z}_p \to R.$$

So consider the ring homomorphism

$$\psi : Z_p[[x_1, \ldots, x_n]] \to R$$

obtained by extending (by linearity)

$$\psi(x_k) = y_k \text{ for all } k = 1, \ldots, n;$$
$$\psi(\alpha) = \iota(\alpha) \text{ for all } \alpha \in \mathbb{Z}_p.$$

You should check this is a well-defined ring homomorphism. We show that ψ is surjective. Given $\beta \in R$, either $\beta \in \mathfrak{m}$ or $\beta \notin \mathfrak{m}$. If $\beta \in \mathfrak{m}$, then there exists $x \in (x_1, \ldots, x_n)$ such that $\psi(x) = \beta$ (check this). If $\beta \notin \mathfrak{m}$ then $\beta \in R^*$ (units of R) and so there exists $\alpha \in \mathbb{Z}_p$ such that $\iota(\alpha) = \beta$ (check this). Hence, if we consider $I = \ker(\psi)$, the first isomorphism theorem gives us

$$R \cong Z_p[[x_1, \ldots, x_n]]/I.$$