Student seminar solutions Week 3

1. We know from lecture that the degree of the extension $F/\mathbb{Q}$ is equal to $[F : \mathbb{Q}] = r + 2s$ where r is the number of real embeddings and s the number of pairs of complex embeddings.
We want to find the embeddings of the field $F = \mathbb{Q}(\sqrt{3}, \sqrt{7})$. First notice that there are embeddings that sends $\sqrt{3} \to \pm\sqrt{3}$ and $\sqrt{7} \to \pm\sqrt{7}$. Choosing every combination of plus and minus makes already 4 differents real embeddings.
Notice that $[F : \mathbb{Q}] \geq 4$ since $1, \sqrt{3}, \sqrt{7}$ and $\sqrt{21}$ are linearly independant (where F is seens as a $\mathbb{Q}-$vector space). Hence $r = 4$ and $s = 0$.
Also from lecture we know that $\mathcal{O}_F^\times = W_F \times \mathbb{Z}^{r+s-1} = W_F \times \mathbb{Z}^3$ where W_F is the group of unity of F (setwise we have $W_F = \mathcal{U}_1 \cap F$ where $\mathcal{U}_1 \subset \mathbb{C}$ is the unit circle). In this case, $W_F \cong \mathbb{Z}/2\mathbb{Z}$ corresponding to $\pm 1 \subset \mathcal{U}_1$.
To find explicit generators of the free part of $\mathcal{O}_F^\times$, we want to find $a, b \in \mathbb{Z}$ such that $a + b\sqrt{d}$ is of norm 1 for $d = 3, 7, 21$. Such integers would satisfy: $1 = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2 d$. Checking for small values of a and b, we find generators: $\{2 + \sqrt{3}, 8 + 3\sqrt{7}, 55 + 12\sqrt{21}\}$.

   Now the same for $F' = \mathbb{Q}(\sqrt{3}, \sqrt{7}, i)$. There are already 4 pairs of complex embeddings that sends $\sqrt{3} \to \pm\sqrt{3}$, $\sqrt{7} \to \pm\sqrt{7}$ and $i \to \pm i$. Again notice that $[F' : \mathbb{Q}] \geq 8$ since $1, \sqrt{3}, \sqrt{7}, \sqrt{21}, i, i\sqrt{3}, i\sqrt{7}$ and $i\sqrt{21}$ are linearly indepedant. Hence $r = 0$ and $s = 4$.
   Notice that $F' \cap \mathcal{U}_1 = \{\pm 1, \pm i\}$ so we have that $W_{F'} = \mathbb{Z}/4\mathbb{Z} \implies \mathcal{O}_{F'}^\times = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}^3$.
   Using the same logic as for the group $\mathcal{O}_F^\times$, we find generators of the free part of the unit group $\mathcal{O}_K^\times$: $\{i, 2 + \sqrt{3}, 8 + 3\sqrt{7}, 55 + 12\sqrt{21}\}$

2. (a) We want to find integers $a_0, a_1, ...$ with $a_i \in \{0, ..., 6\}$ such that

$$\frac{1}{6} = a_0 + a_1 7 + a_2 7^2 + a_3 7^3 + ...$$

   We begin with a_0, it must satisfy $6a_0 \equiv 1 \pmod 7$. Since $6^2 = 36 \equiv 1 \pmod 7$, we have that $a_0 = 6$.
   Next, a_1 must satisfy $6(6 + 7a_1) \equiv 1 \pmod{49} \iff 36 + 42a_1 \equiv 1 \pmod{49} \iff 42a_1 \equiv -35 \equiv 14 \pmod{49}$. Dividing by 7 we have

$$6a_1 \equiv 2 \pmod 7 \iff a_1 \equiv 6^{-1} \cdot 2 \equiv 6 \cdot 2 \equiv 5 \pmod 7$$

Going on we look for a_3 satisfying $6(6+7\cdot 6+7^2a_3)\equiv 1 \pmod{7^3}$ and after the computation we find $a_3=5$. We begin to see a pattern and we suggest that $\frac{1}{6}=6555...=6\bar{5}$ in 7-addic expansion. Now we can check the result:

$$6555...=6+5\cdot 7+5\cdot 7^2+...=6+5\sum_{k\geq 1}7^k=6+5\frac{7}{1-7}=6-\frac{35}{6}=\frac{36-35}{6}=\frac{1}{6}$$

(b) Reformulating the question, we want to find for which prime p between 2 and 13 does the polynomial $P(X)=X^2+1\in\mathbb{Z}_p[X]$ have a root in $\mathbb{Q}_p$. A root α of P would be in $\mathbb{Z}_p$ since $1=|-1|_p=|\alpha^2|_p=|\alpha|_p^2$ by multiplicity of the norm.

Using Hensel's lemma, if the reduction of P in the ring $\mathbb{Z}/p\mathbb{Z}[X]$ has a root $\bar{\alpha}$ that is simple, then it lifts to a root α of P in $\mathbb{Z}_p[X]$. Hence since $(X+2)(X+3)=X^2+1 \pmod 5$ and $(X+5)(X+8)=X^2+1 \pmod{13}$ then $\mathbb{Z}_5$ and $\mathbb{Z}_{13}$ have square roots of -1.

Then notice that if P has a root in $\mathbb{Z}_p$ so that $P(X)=(X-\alpha)(X-\beta)$, with $\alpha,\beta\in\mathbb{Z}_p$ then looking at the reduction modulo p we have that $\bar{P}(X)=(X-\bar{\alpha})(X-\bar{\beta})\in\mathbb{Z}/p\mathbb{Z}[X]$ has roots in $\mathbb{Z}/p\mathbb{Z}[X]$.
For $p=3,7,11$, since $\bar{P}(X)=X^2+1$ is irreducible in $\mathbb{Z}/p\mathbb{Z}[X]$ (after quickly checking manually), we find that -1 isn't a square in $\mathbb{Z}_p$.

Now suppose that P has a root in $\mathbb{Z}_2$, then its reduction in $\mathbb{Z}/p\mathbb{Z}[X]$ but also in $\mathbb{Z}/p^n\mathbb{Z}[X]$ (for any $n\in\mathbb{N}$) should have a root. However the polynomial $\bar{P}(X)=X^2+1\in\mathbb{Z}/4\mathbb{Z}[X]$ is irreducible, contradiction.

Hence the only p where -1 has a root is 5 and 13.

3. Suppose that the 2 norms are equivalent, i.e that there are real numbers $c,C\in\mathbb{R}$ such that $c|y|_{\mathfrak{p}}\leq|y|_{\mathfrak{q}}\leq C|y|_{\mathfrak{p}}$ for every $y\in F$.
Since $\mathfrak{p}\neq\mathfrak{q}$, there is an element $x\in\mathfrak{p}\backslash\mathfrak{q}$. Then for $\epsilon\in\mathbb{N}, x^n\in\mathfrak{p}^n$, so $|x^n|_{\mathfrak{p}}=\epsilon^n$ and $|x|_{\mathfrak{q}}=\epsilon$ for some $0\leq\epsilon\leq 1$, therefore:

$$c|x^n|_{\mathfrak{p}}\leq|x^n|_{\mathfrak{q}}\leq C|x^n|_{\mathfrak{p}}\iff c\epsilon^n\leq\epsilon\leq C\epsilon^n$$

And for $n>>1$ big integer we have that $\epsilon\geq C\epsilon^n$, a contradiction.

4. Let $\mathfrak{p}\mathcal{O}_K=\mathfrak{B}^e{\mathfrak{B}_1}^{e_1}\cdots{\mathfrak{B}_{\mathfrak{g}}}^{e_g}$ with $\mathfrak{B}_i\subset\mathcal{O}_K$ prime ideals the decomposition into prime ideal. We choose uniformizers $\pi_{\mathfrak{p}}\in F,\pi_{\mathfrak{B}}\in K$ such that $\pi_{\mathfrak{p}}\in\mathfrak{p}\backslash\mathfrak{p}^2,\pi_{\mathfrak{B}}\in\mathfrak{B}\backslash\mathfrak{B}^2$.
Therefore there is an ideal $I\subset\mathcal{O}_F$ coprime to $\mathfrak{p}$ such that $\pi_{\mathfrak{p}}\mathcal{O}_F=\mathfrak{p}I$. We then have $\pi_{\mathfrak{p}}\mathcal{O}_K=(\pi_{\mathfrak{p}}\mathcal{O}_F)\mathcal{O}_K=\mathfrak{p}I\mathcal{O}_K\cong(\mathfrak{p}\mathcal{O}_K)(I\mathcal{O}_K)=\mathfrak{B}^e{\mathfrak{B}_1}^{e_1}\cdots{\mathfrak{B}_{\mathfrak{g}}}^{e_g}I\mathcal{O}_K$ with $I\mathcal{O}_K$ coprime to $\mathfrak{B}^e\mathfrak{B}_1^{e_1}\cdots\mathfrak{B}_g^{e_g}$. Since $\pi_{\mathfrak{B}}\in$

$\mathfrak{B}\backslash\mathfrak{B}^2 \subset \mathcal{O}_K$ is a uniformizer, we have that $\pi_{\mathfrak{B}}\mathcal{O}_K = \mathfrak{B}J$ with J and $\mathfrak{B}$ coprime.
Hence we have that $|\pi_{\mathfrak{B}}|_{\mathfrak{B}}^{e} = |\pi_{\mathfrak{p}}|_{\mathfrak{B}}$.