Mathematics GR6657 Algebraic Number Theory
Assignment # 1

Benjamin Church

February 9, 2022

1. (a) Let V be a finite-dimensional $\mathbb{Q}_p$-vectorspace with a norm $|\bullet|_V$ such that for $v \in V$ and $a \in \mathbb{Q}_p$ we have $|av|_V = |a|_p|v|_V$. Then, let $v_1, \cdots, v_r$ be a basis of V and define the supremum norm,

$$\left|\left|\sum_{i=1}^{r} c_i v_i\right|\right| = \sup_{1\leq i\leq r} |c_i|_p$$

This norm agrees with $|\bullet|_V$ (up to the scalar $|v_i|_V$) on the subspace spanned by v_i which is a copy of $\mathbb{Q}_p$ inside V. Therefore, the two norms are equivalent on V i.e. there exist nonzero constants C and C' such that,

$$C||v|| \leq |v|_V \leq C'||v||$$

We must show that V is complete with respect to $|\bullet|_V$. Given a Cauchy sequence $\{u^{(i)}\}$, we write it in components with respect to the basis $\{v_i\}$. That is, from $\{u^{(i)}\}$ we get n sequences of the form $\{u_j^{(i)}\}$ with $u_j^{(i)} \in \mathbb{Q}_p$ such that,

$$\sum_{j=1}^{r} u_j^{(i)} v_j = u^{(i)}$$

Because the sequence is Cauchy, for any $\varepsilon > 0$ there exists some N such that for $n, m > N$ we have,

$$C|u_j^{(n)} - u_j^{(m)}|_p \leq C||u^{(n)} - u^{(m)}|| \leq |u^{(n)} - u^{(m)}|_V < \varepsilon$$

for any $1 \leq j \leq r$. Therefore, each sequence $\{u_j^{(i)}\}$ is also Cauchy because,

$$|u_j^{(n)} - u_j^{(m)}|_p < \frac{\varepsilon}{C}$$

By the completeness of $\mathbb{Q}_p$, each of these sequences has a limit, $u_j = \lim_{n\to\infty} u_j^{(n)}$. Define $u = \sum_{i=1}^{r} u_i v_i$. Then, for any $\varepsilon > 0$ there exists N_j such that $n > N_j \implies |u_j^{(n)} - u_j|_p < \epsilon$. Therefore, for $n > \sup_{1\leq i\leq r} N_i$, we have,

$$|u^{(i)} - u|_V \leq C'||u^{(i)} - u|| \leq \sup_{1\leq j\leq r} |u_j^{(i)} - u_j|_p < \varepsilon$$

so $\lim_{n\to\infty} u^{(n)} = u$. Therefore, V is complete with respect to the norm $|\bullet|_V$.

(b) Let K be a field of characteristic zero and therefore there is an embedding $\iota : \mathbb{Q} \to K$. Futhermore, suppose that K is complete with respect to $||\bullet||$ such that $||\iota(a)|| = |a|_p$ for any $a \in \mathbb{Q}$. The embedding map extends to $\iota : \mathbb{Q}_p \to K$ by,

$$\iota(\lim_{n\to\infty} a_n) = \lim_{n\to\infty} \iota(a_n)$$

This is defined on all of $\mathbb{Q}_p$ because any element of $\mathbb{Q}_p$ can be written as the limit of a cauchy sequence whose terms are in $\mathbb{Q}$. Also, if

$$\lim_{n\to\infty} a_n = \lim_{n\to\infty b_n}$$

for two sequences $a_n, b_n \in \mathbb{Q}$ then,

$$||\iota(a_n) - \iota(b_n)|| = ||\iota(a_n - b_n)|| = |a_n - b_n|_p \to 0$$

so $\iota(\lim_{n\to\infty} a_n) = \iota(\lim_{n\to\infty} b_n)$ which means that ι is well-defined. Furthermore, because the norm on a_n is preserved under ι which is a homomorphism so $\iota(a_n)$ is also Cauchy ($|a_n - a_m|_p = ||\iota(a_n - a_m)|| = ||\iota(a_n) - \iota(a_m)||$) and K is complete so the limit exists. It suffices to show that ι is a continuous homomorphism,

$$\iota(\lim_{n\to\infty} a_n + b_n) = \lim_{n\to\infty} \iota(a_n + b_n) = \lim_{n\to\infty} [\iota(a_n) + \iota(b_n)] = \lim_{n\to\infty} \iota(a_n) + \lim_{n\to\infty} \iota(b_n)$$

and

$$\iota(\lim_{n\to\infty} a_n b_n) = \lim_{n\to\infty} \iota(a_n + b_n) = \lim_{n\to\infty} [\iota(a_n)\iota(b_n)] = \left(\lim_{n\to\infty} \iota(a_n)\right)\left(\lim_{n\to\infty} \iota(b_n)\right)$$

Furthermore, $||\iota(a)|| = |a|_p$ for any $a \in \mathbb{Q}_p$ so if $\lim_{n\to\infty} a_n = a$ for any sequence $a_n \in \mathbb{Q}_p$, then for any ε, there exists N such that for $n > N$,

$$||\iota(a_n) - \iota(a)|| = |a_n - a|_p < \varepsilon$$

so $\lim_{n\to\infty} \iota(a_n) = \iota(a)$ and thus ι is continuous.

2. We consider quadratic extensions of $\mathbb{Q}_p$. As proven in class, every finite extension of $\mathbb{Q}_p$ is generated by an element of $\mathbb{Q}$. Thus, we can restrict our study to extensions of the form $\mathbb{Q}_p(\sqrt{d})$ where $d \in \mathbb{Q}$.

(a) Take $p \neq 2$. Any quadratic extension of $\mathbb{Q}_p$ is of the form, $\mathbb{Q}_p(\sqrt{d})$. First, suppose $\left(\frac{d}{p}\right) = 1$ then, d is a square modulo p so $x^2 - d$ has a root in $\mathbb{F}_p \cong \mathbb{Q}_p/\mathbb{Z}_p$ and $(x^2 - d)' = 2d \equiv 0 \pmod p$ because $p \neq 2$ so by Hensel's lemma $x^2 - d$ has a root in $\mathbb{Q}_p$. Thus, $\mathbb{Q}_p(\sqrt{d}) = \mathbb{Q}_p$. Else, suppose that $\left(\frac{d}{p}\right) = -1$ then d cannot have a root in $\mathbb{Q}_p$ because otherwise its image in $\mathbb{Q}_p/\mathbb{Z}_p$ would be a root of $x^2 - d$ in $\mathbb{F}_p$ which does not exist. Thus, $\mathbb{Q}_p(\sqrt{d}) \neq \mathbb{Q}_p$. However, the product of two nonresidues is a residue so if $\left(\frac{d}{p}\right) = \left(\frac{d'}{p}\right)$ then $\left(\frac{dd'}{p}\right) = 1$ and thus dd' is a square in $\mathbb{Q}_p$ so $dd' = a^2$ and thus $d' = \frac{a^2}{d}$ so $\mathbb{Q}_p(\sqrt{d}) = \mathbb{Q}_p(\sqrt{d'})$. Therefore, there is exactly one quadratic extension of $\mathbb{Q}_p$ generated by a nonresidue.

Next, take $d = p$. We know that p is not a square in $\mathbb{Q}_p$ because p is a uniformizer.

Thus, $\mathbb{Q}_p(\sqrt{p}) \neq \mathbb{Q}_p$. Furthermore, p is ramified in $\mathbb{Q}_p(\sqrt{p})$ but unramified in $\mathbb{Q}_p(\sqrt{d})$ since $ef = 2$ but $f > 1$ because $k(\mathbb{Q}_p(\sqrt{d}) \supset \mathbb{F}_p[\sqrt{d}] \supsetneq \mathbb{F}_p$ because d is a nonresidue. Therefore, $\mathbb{Q}_p(\sqrt{p}) \neq \mathbb{Q}_p(\sqrt{d}) \neq \mathbb{Q}_p$.

Finally, consider $p \mid d$ but $p \neq d$. Take $d = pk$. Since d can be choosen to be square-free, we require $p \nmid k$. Thus, if k is a quadratic residue modulo p then k is a square in $\mathbb{Q}_p$ so d is not squre-free. Therefore, take k to be a nonresidue. In this case, all such $\mathbb{Q}_p(\sqrt{pk})$ are equivalent because any two nonresidues differ by a square in $\mathbb{Q}_p$. Futhermore, suppose that $\mathbb{Q}_p(\sqrt{d}) = \mathbb{Q}_p(\sqrt{pk})$ then pkd is a square but k and d are nonresidues so kd is a square in $\mathbb{Q}_p$. Thus, p must be a square which contradicts the fact that $\mathbb{Q}_p(\sqrt{d}) \neq \mathbb{Q}_p(\sqrt{p})$. Finally, if $\mathbb{Q}_p(\sqrt{p}) = \mathbb{Q}_p(\sqrt{pk})$ then both p and pk are square which implies that k is a square, again contradicting the fact that $\mathbb{Q}_p(\sqrt{d}) \neq \mathbb{Q}_p(\sqrt{p})$. Thus, $\mathbb{Q}_p(\sqrt{pk})$ is distinct from any of the quadratic fields so far constructed. Also, $p \nmid k$ so $k \in \mathbb{Q}_p^\times$ so $(\sqrt{pk})^2 = (p)$ and thus p is ramified in $\mathbb{Q}_p(\sqrt{pk})$. In particular, $\mathbb{Q}_p(\sqrt{pk}) \neq \mathbb{Q}_p$. Thus, there are exactly 3 quadratic extensions of $\mathbb{Q}_p$. These are,

$$\mathbb{Q}_p(\sqrt{d}) \quad \mathbb{Q}_p(\sqrt{p}) \quad \mathbb{Q}_p(\sqrt{pd})$$

where d is any quadratic nonresidue modulo p.

(b) The classification of quadratic extensions of $\mathbb{Q}_2$ follows from an important lemma from elementary number theory,

Lemma 0.1. *Let d be odd, d is a quadratic residue modulo 2^r for every $r \in \mathbb{Z}^+$ if and only if $d \equiv 1 \pmod 8$.*

By the inverse limit construction of $\mathbb{Z}_2$, a number $d \in \mathbb{Q}$ is a square in $\mathbb{Z}_p$ if and only if its reduction to $\mathbb{Z}/2^r\mathbb{Z}$ is a square for every r. Therefore, for $2 \nmid d$, the field $\mathbb{Q}_2(\sqrt{d})$ is a quadratic extension of $\mathbb{Q}_p$ if and only if $d \not\equiv 1 \pmod 8$ such that $x^2 - d$ has no roots (in particular) modulo 8 and thus no roots in $\mathbb{Q}_2$. Furthermore, for two odd d, d' i.e. $d, d' \in (\mathbb{Z}/8\mathbb{Z})^\times$, the following are equivalent,

$$d \equiv d' \pmod 8 \iff d^{-1}d' \equiv 1 \pmod 8 \iff d^{-1}d' \in (\mathbb{Q}_2)^2 \iff \mathbb{Q}_2(\sqrt{d}) = \mathbb{Q}_2(\sqrt{d'})$$

Therefore, the quadratic extensions $\mathbb{Q}_2(\sqrt{d})$ with odd d are in one-to-one correspondence with the nontrivial elements of $(\mathbb{Z}/8\mathbb{Z})^\times$. Thus, we can choose representatives,

$$\mathbb{Q}_2(\sqrt{3}) \quad \mathbb{Q}_2(\sqrt{5}) \quad \mathbb{Q}_2(\sqrt{7})$$

for the set of all quadratic extensions of $\mathbb{Q}_2$ by odd d.

Now we consider $\mathbb{Q}_p(\sqrt{d})$ for even d. Write $d = 2k$ with $2 \nmid k$ because we can take d to be square-free since $\mathbb{Q}_2(\sqrt{a^2k}) = \mathbb{Q}_2(\sqrt{k})$. Using the same argument as above,

$$k \equiv k' \pmod 8 \iff k^{-1}k' \equiv 1 \pmod 8 \iff k^{-1}k' \in (\mathbb{Q}_2)^2 \iff \mathbb{Q}_2(\sqrt{2k}) = \mathbb{Q}_2(\sqrt{2k'})$$

However, $\mathbb{Q}_2(\sqrt{2k}) \neq \mathbb{Q}_p$ because $2 \nmid k$ so k is a unit in $\mathbb{Q}_2$. Thus, $(\sqrt{2k})^2 = (2k) = (2)$ so $2k$ cannot be a square in $\mathbb{Q}_2$ because 2 is a uniformizer for the prime ideal (2) in $\mathbb{Z}_2$. Therefore, the quadratic extensions $\mathbb{Q}_2(\sqrt{d})$ with even d are in one-to-one correspondence with *all* elements of $(\mathbb{Z}/8\mathbb{Z})^\times$ with representatives,

$$\mathbb{Q}_2(\sqrt{2}) \quad \mathbb{Q}_2(\sqrt{6}) \quad \mathbb{Q}_2(\sqrt{10}) \quad \mathbb{Q}_2(\sqrt{14})$$

However, if $\sqrt{d} = a + b\sqrt{2k}$ then $d = a^2 + 2kb^2 + 2ab\sqrt{2k}$ so $a = 0$ or $b = 0$ which either way implies that d is a square or d is even. Thus, the quadratic extensions derived from the two different case must be distinct. Thus, in total, there are 7 distinct quadratic extensions of $\mathbb{Q}_2$.

3. Let L/K be an extension of p-adic fields and let Π be a uniformizer of L with $\mathfrak{m}_L = (\Pi)$ and π a uniformizer of K with $\mathfrak{m}_K = (\pi)$ such that $\mathfrak{m}_K\mathcal{O}_L = (\Pi)^e$.

   (a) Define the groups,

   $$I_i = \{g \in Gal(L/K) \mid \ g(a) \equiv a \,(\mathrm{mod}\, \mathfrak{m}_L^{i+1}) \,\}$$

   take $g \in I_0 = I$ then we know that g permutes prime ideals. However, $\mathcal{O}_L$ is a DVR so it has a unique prime ideal. Thus, $g(\mathfrak{m}_L) = \mathfrak{m}_L$ so $(g(\Pi)) = (\Pi)$ which implies that $g(\Pi) = u\Pi$ where u is a unit. Let $\alpha(g)$ be the image of u in $k(L)^\times = (\mathcal{O}_L/\mathfrak{m}_L)^\times$ which is nonzero because u is invertable in $k(L)$. Thus, $u \equiv \alpha(g) \,(\mathrm{mod}\, \mathfrak{m}_L)$ so,

   $$g(\Pi) \equiv \alpha(g)\Pi \,(\mathrm{mod}\, \mathfrak{m}_L^2)$$

   Then, Furthermore, let $g, h \in I$ then consider,

   $$g \circ h(\Pi) \equiv \alpha(g \circ h)\Pi \,(\mathrm{mod}\, \mathfrak{m}_L^2)$$

   However,

   $$g(\Pi) \equiv \alpha(g)\Pi \,(\mathrm{mod}\, \mathfrak{m}_L^2) \qquad h(\Pi) \equiv \alpha(h)\Pi \,(\mathrm{mod}\, \mathfrak{m}_L^2)$$

   Therefore,

   $$(g \circ h)(\Pi) \equiv g(\alpha(h)\Pi) = g(\alpha(h))g(\Pi) \equiv \alpha(g)g(\alpha(h))\Pi \equiv \alpha(g)\alpha(h)\Pi \ \,(\mathrm{mod}\, \mathfrak{m}_L^2)$$

   where I have used the fact that $g \in I$ so $g(\alpha(h)) \equiv \alpha(h) \,(\mathrm{mod}\, \mathfrak{m}_L)$. Therefore, the map, $\alpha : I \to k(L)^\times$ is a homomorphism.

   Now, we will show that $\ker \alpha = I_1$. First, if $g \in I_1$ then by definition, $g(\Pi) \equiv \Pi \,(\mathrm{mod}\, \mathfrak{m}_L^2)$ so $g \in \ker \alpha$. Conversely, suppose that $g \in \ker \alpha$ then, $g \in I$ and $g(\Pi) \equiv \Pi \,(\mathrm{mod}\, \mathfrak{m}_L^2)$. Any $a \in \mathcal{O}_K$ can be written as $a = \sum_{i \geq 0} a_i \Pi^i$ with $a_i \in k(L)$. Thus,

   $$g(a) = \sum_{i \geq 0} g(a_i)g(\Pi)^i \equiv \sum_{i \geq 0} a_i \Pi^i = a \ \,(\mathrm{mod}\, \mathfrak{m}_L^2)$$

   thus, $g \in I_1$ so $\ker \alpha = I_1$. Since the map $\alpha : I \to k(L)^\times$ is a homomorphism, the map decends to an injective homomorphism, $\alpha : I/I_1 \to k(L)^\times$. In particular, I/I_1 is isomorphic to a subgroup of $k(L)^\times$ which has order $q - 1 = p^f - 1$. Therefore, by Lagrange's theorem, I/I_1 has order dividing $p^f - 1$ which must thus be coprime to p.

   (b) For $i > 0$ define the map $\alpha : I_i \to k(L)$ by,

   $$g(\Pi) \equiv \Pi + \alpha(g)\Pi^{i+1} \,(\mathrm{mod}\, \mathfrak{m}_L^{i+2})$$

   This map is well defined because $g \in I_i$ so $g(\Pi) \equiv \Pi \,(\mathrm{mod}\, \mathfrak{m}_L^{i+1})$ so $g(\Pi) = \Pi + a\Pi^{i+1}$. For $g, h \in I_i$ consider,

   $$(g \circ h)(\Pi) \equiv g(\Pi) + g(\alpha(h))g(\Pi)^{i+1} \equiv \Pi + \alpha(g)\Pi^{i+1} + \alpha(h)\Pi^{i+1} \ \,(\mathrm{mod}\, \mathfrak{m}_L^{i+2})$$

because g fixes $k(L)$ and preserves Π^{i+1} modulo Π^{i+2} since

$$g(\Pi)^{i+1} = (\Pi + \alpha(g)\Pi^{i+1} + r\Pi^{i+2})^{i+1} = \Pi^{i+1} + (i+1)\alpha(g)\Pi^{2i+2} + \cdots$$

Thus, $\alpha(g \circ h) = \alpha(g) + \alpha(h)$ so α is a homomorphism. Furthermore, if $g \in I_{i+1}$ then,

$$g(\Pi) \equiv \Pi \pmod{\mathfrak{m}_L^{i+2}}$$

so $g \in \ker \alpha$. Conversely, if $g \in \ker \alpha$ then g preserves Π modulo $\mathfrak{m}_L^{i+2}$ i.e.

$$g(\Pi) \equiv \Pi \pmod{\mathfrak{m}_L^{i+2}}$$

But any element $a \in \mathcal{O}_L$ can be written as $\sum_{i \geq 0} a_i \Pi^i$ with $a_i \in k(L)$. But g fixes $k(L)$ so,

$$g(a) = \sum_{i \geq 0} g(a_i) g(\Pi)^i \equiv \sum_{i \geq 0} a_i \Pi^i = a \pmod{\mathfrak{m}_L^{i+2}}$$

Thus, for any $a \in \mathcal{O}_L$ we have, $g(a) \equiv a \pmod{\mathfrak{m}_L^{i+2}}$ so $g \in I_{i+1}$. Thus, $\ker \alpha = I_{i+1}$. Because $\alpha : I_i \to k(L)$ is a homomorphism with kernel I_{i+1}, α decends to an injective homomorphism $\alpha : I_i/I_{i+1} \to k(L)$. Thus, I_i/I_{i+1} is embedded in the additive group $k(L)$ which has order p^f. By Lagrange's theorem, I_i/I_{i+1} has order p^k for some $k \leq f$.

For any $g \in Gal(L/K)$, consider $a = g(\Pi) - \Pi$. If a were a unit then since $(g(\Pi)) = (\Pi)$ we would have $a \in \mathfrak{m}_L$ so $\mathfrak{m}_L = \mathcal{O}_L$ which is a contradiction. Thus, if $a \neq 0$ i.e. $g \neq \mathrm{id}$ then by Dedekind prime factorization, $(a) = \mathfrak{m}_L^k$ for some k. Thus, $g \in I_i$ for $i < k$ but by the uniqueness of prime ideal factorization, $g \notin I_k$. Therefore, because $Gal(L/K)$ is finite, the chain of subgroups,

$$I_0 \supset I_1 \supset I_2 \supset \cdots$$

must terminate at some $I_N = \{\mathrm{id}_L\}$ since every element has a maximum index at which it appears in the sequence. Furthermore,

$$|I_1| = \left(\prod_{i=1}^{N-1} |I_i|/|I_{i+1}| \right) \cdot |I_N| = \left(\prod_{i=1}^{N-1} |I_i/I_{i+1}| \right) \cdot |I_N| = \prod_{i=1}^{N-1} |I_i/I_{i+1}|$$

but each factor group is a p-group. Thus, I_1 is a p-group.

(c) Let K be a p-adic field and consider the extension $K(\sqrt[d]{\pi})$ where $q = |k(K)|$ and $d \mid q-1$. First, I will argue that $x^d - \pi$ splits completely in K. The polynomial $x^d - 1$ has a root in $k(K) \cong \mathbb{F}_q$ because $\mathbb{F}_q^\times$ is cyclic so let $g \in k(K)$ have order $q-1$. Then, since $d \mid q-1$, take $x = g^{\frac{q-1}{d}}$ such that $x^d - 1 = 0$ and x is a primitive d^{th}-root of unity. Because $(x^d - 1)' = dx^{d-1} \neq 0$ in $k(K)$ then by Hensel's lemma, there exists a root ω of $x^d - 1$ in K such that $\omega \equiv x \pmod{\mathfrak{m}_L}$. Thus, K contains d, d^{th}-root of unity. Thus, the we can factor the polynomial,

$$x^d - \pi = (x - \sqrt[d]{\pi})(x - \omega\sqrt[d]{\pi}) \cdots (x - \omega^{d-1}\sqrt[d]{\pi})$$

Thus, $K(\sqrt[d]{\pi})$ is the splitting field of $x^d - \pi$ over K and therefore Galois because K has characteristic zero. By the Cyclic Extension theorem, since K contains all d^{th}-roots

of unity and $(\sqrt[d]{\pi})^d = \pi \in K$, we have that $K(\sqrt[d]{\pi})/K$ is a cyclic extension and thus abelian. Futhermore, with $L = K(\sqrt[d]{\pi})$, the ideal $\mathfrak{m}_K\mathcal{O}_L = \pi\mathcal{O}_L = (\sqrt[d]{\pi})^d$. Therefore, the ramification index must be at least d. However, $n = [L : K] = d$ because $x^d - \pi$ is irreducible in K else π could not be a uniformizer. Thus, $e = d = n$ so L/K is totally ramified. Furthermore, $e = d$ and $d \mid q - 1$ with $q = p^f$ by assumption. Thus, $p \nmid d$ since $p \nmid q - 1$. Therefore, $p \nmid e$ since $e = d$. Therefore, L/K is tamely and totally ramified.