

Math 6122: In class worksheet/HW 2

Due: Thursday, January 24th, start of class

1. Let F be a field of characteristic not 2, and let $F^* = F \setminus \{0\}$. Show that every quadratic extension of F is of the form $F(\sqrt{D})$ for some D that is not in $(F^*)^2$ (subgroup of squares of the multiplicative group F^*), and that the extension only depends on the class of D in $F^*/(F^*)^2$, i.e., quadratic extensions are in bijection with non-identity elements of the group $F^*/(F^*)^2$.
2.
 - Let $F := \mathbb{F}_q$ be a finite field of odd characteristic, and let $F^* = F \setminus \{0\}$. Show that the group $F^*/(F^*)^2 \cong \mathbb{Z}/2\mathbb{Z}$ and use this to show that there is exactly one quadratic extension of the field F .
 - Show that the polynomial $(x^2 - 2)(x^2 - 3)(x^2 - 6)$ has a root in \mathbb{F}_p for every prime p but has no roots in \mathbb{Z} .

[Reading exercise: In fact, a finite field F has exactly one extension of every degree. Fix a degree n and let F_n be the unique extension of degree n . Is this extension Galois? What is the Galois group? Answers in Section 14.3 of Dummit and Foote, but try to see if you can guess enough automorphisms on your own. Hint: Finite fields have a special field automorphism called the Frobenius $x \rightarrow x^q$ – why does this respect addition, and what is its order in $\text{Gal}(E/F)$ if $[E : F] = n$?

We will now construct a fun new field called the p -adic numbers, and show that it has exactly 3 quadratic extensions when p is odd. Contrast this with \mathbb{Q} which has infinitely many distinct quadratic extensions (we know this from Problem 1– why?).

Let p be a prime number. Let $\mathbb{Z}_p := \{(z_n)_{n \geq 1} \in \prod_{n \geq 1} \mathbb{Z}/p^n\mathbb{Z} \mid z_{n+1} \cong z_n \pmod{p^n} \forall n\}$. The set \mathbb{Z}_p is in fact a subring of the infinite product ring that contains \mathbb{Z} (integer a embedded diagonally as $(a \pmod{p^n})$), and one way to represent elements in this ring is a “power series in the variable p ”, which we shall now explain. Every congruence class in $\mathbb{Z}/p^n\mathbb{Z}$ can be represented using a unique integer z_n in the range $0 \leq z_n \leq p^n - 1$, which can further be written in terms of its base p expansion $z_n = \sum_{i=0}^{n-1} a_i p^i$ for integers a_i satisfying $0 \leq a_i \leq p - 1$ (z_n uniquely determines the digits a_0, a_1, \dots, a_{n-1} and vice versa). Check the set of compatible z_{n+1} for a given z_n , i.e.

$$\{z_{n+1} \pmod{p^{n+1}} \mathbb{Z} \mid z_{n+1} \cong z_n \pmod{p^n}\mathbb{Z}\} = \{z_n + a_n p^n \mid 0 \leq a_n \leq p - 1\}.$$

This means that every element of \mathbb{Z}_p has a unique representation of the form $z = \sum_{i \geq 0} a_i p^i$ for some integers a_i in the range $0 \leq a_i \leq p - 1$, by which we mean $z_n = \sum_{i=0}^{n-1} a_i p^i$ defines a

compatible sequence. (What's the p -adic expansion of -1 ???) **WARNING:** One should be careful while adding and multiplying elements using their unique power series representation, since addition and multiplication are defined with “carry” operations.

Tool to visualize \mathbb{Z}_p : We can also visualize elements of \mathbb{Z}_p as infinite paths in a complete rooted p -ary tree! Here is the complete binary tree that shows up for \mathbb{Z}_2 . The nodes at depth i of the tree correspond to congruence classes of \mathbb{Z} modulo $2^i\mathbb{Z}$. So there is one node at depth 0, which is a root, 2 nodes at depth 1, 4 nodes at depth 2, 8 nodes at depth 3 and so on. A node at depth $n+1$ (corresponding to the congruence class $z_{n+1} \bmod 2^{n+1}\mathbb{Z}$) is a child of a node at depth n (corresponding to the congruence class $z_n \bmod 2^n\mathbb{Z}$) if and only if $z_{n+1} \cong z_n \bmod 2^n\mathbb{Z}$. Going back, there are two nodes at depth 1 corresponding to the classes of odd integers and even integers. The two children of the even integers at depth 2 correspond to the classes $0 + 0.2^1 \bmod 2^2$ and $0 + 1.2^1 \bmod 2^2$, i.e. $0 \bmod 4$ and $2 \bmod 4$, and similarly the children of the odd integers at depth 2 are the congruence classes $1 + 0.2^1 \bmod 2^2$ and $1 + 1.2^1 \bmod 2^2$, i.e. $1 \bmod 4$ and $3 \bmod 4$. The two children of the class $2 \bmod 4$ at depth 3 are $2 + 0.2^2 \bmod 2^3$ and $2 + 1.2^2 \bmod 2^3$, i.e. $2 \bmod 8$ and $6 \bmod 8$ and so on... Draw the first four levels of this binary tree! Do you now see why infinite paths from the root down this tree correspond to elements of \mathbb{Z}_2 ?

For the rest of the problem assume that p is an odd prime.

3. Define the valuation map $\text{ord}_p: \mathbb{Z}_p \setminus \{0\} \rightarrow \mathbb{Z}$ by

$$\text{ord}_p((z_n)) = \max\{n \mid z_n = 0 \bmod p^n\mathbb{Z}\}.$$

Show that $\text{ord}_p((z_n w_n)) = \text{ord}_p((z_n)) + \text{ord}_p((w_n))$.

4. Let $z = (z_n)$ and $w = (w_n)$ be two nonzero elements of \mathbb{Z}_p . Show that z divides w in \mathbb{Z}_p if and only $\text{ord}_p z \leq \text{ord}_p w$. Conclude that the units in \mathbb{Z}_p are exactly the kernel of ord_p , and that \mathbb{Z}_p is an integral domain. [Hint: Assume $\text{ord}_p z \leq \text{ord}_p w$ and construct $u = (u_n)$ such that $zu = w$ by induction on n .]
5. Show that \mathbb{Z}_p is a principal ideal domain by showing that every ideal I is generated by an element of smallest valuation in the ideal.
6. Use the natural projection ring homomorphism $\prod_{n \geq 1} \mathbb{Z}/p^n\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z} := \mathbb{F}_p$ to show that if a unit $z = (z_n)$ of the ring \mathbb{Z}_p is in the subgroup of squares, then $z_0 \in (\mathbb{F}_p^*)^2$.
7. Now assume that $z = (z_n) \in \mathbb{Z}_p \setminus \{0\}$ with $\text{ord}_p z = m$. Show that there is a $w = (w_n) \in \mathbb{Z}_p$ with $w^2 = z$ if and only if m is even and $w = p^m u$ for some unit $u = (u_n) \in \mathbb{Z}_p$ with $u_0 \in (\mathbb{F}_p^*)^2$. [Hint: Construct the w_n by induction on n .]
8. Let \mathbb{Q}_p be the fraction field of the integral domain \mathbb{Z}_p . Using the description of units from above, convince yourself that every element of \mathbb{Q}_p is of the form $p^m u$ for some integer m and unit u in \mathbb{Z}_p . Let $\mathbb{Q}_p^* = \mathbb{Q}_p \setminus \{0\}$. Use the previous parts to show that $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and explicitly describe such an isomorphism.
9. Use the previous part to conclude that \mathbb{Q}_p has exactly 3 quadratic extensions – can you say what they are explicitly?

Math 6122 - Homework 2

Caitlin Beecham (Discussed with Anna and Skye)

January 23, 2019

4

We first show that $z|w$ implies that $\text{ord}(z) \leq \text{ord}(w)$. Now, $z|w$ means that $w = sz$. Say we write $s = \sum_{i \geq 0} c_i p^i$, $z = \sum_{i \geq 0} b_i p^i$, and $w = \sum_{i \geq 0} a_i p^i$. Then, $w = \sum_{n \geq 0} a_n p^n = sz = \sum_{n \geq 0} ((\sum_{i=0}^n c_i b_{n-i}) p^n)$. We want to show that $\text{ord}(z) \leq \text{ord}(w)$. This is true if and only if $(b_l = 0 \text{ for all } l < \text{ord}(z) =: m \text{ implies that } a_l = 0 \text{ for all } l < \text{ord}(z))$. Now, assume $b_l = 0$ for all $l < m$, then $a_l = \sum_{i=0}^l b_i c_{l-i} = \sum_{i=0}^l 0 = 0$ for all $l < m$, and we are done. Now, we wish to prove that if $\text{ord}(z) \leq \text{ord}(w)$, then $z|w$. We do so by constructing an $s = (s_n) \in \mathbb{Z}_p$ such that $zs = w$ by induction on n . First, we let $m := \text{ord}(z)$. Then, define $z' = zp^{-m}$ and $w' = wp^{-m}$. Clearly, $zs = w$ if and only if $z's = w'$. So, we inductively construct s such that $z's = w'$. First, we write $w' = \sum_{i \geq 0} a_i p^i$, $z' = \sum_{i \geq 0} b_i p^i$, and $s = \sum_{i \geq 0} c_i p^i$. Then, $w' = sz' = \sum_{n \geq 0} a_n p^n = \sum_{n \geq 0} ((\sum_{i=0}^n c_i b_{n-i}) p^n)$. So, for our base case, we set $c_0 = \frac{a_0}{b_0}$. Then, we inductively assume that we have chosen c_l such that $a_l = \sum_{i=0}^l c_i b_{l-i}$ for all $l \leq n-1$. Now, we wish to choose c_n such that $a_n = \sum_{i=0}^n c_i b_{n-i}$. Well, note that $a_n = (\sum_{i=0}^{n-1} c_i b_{n-i}) + c_n b_0$. So, we let $c_n = \frac{a_n - \sum_{i=0}^{n-1} c_i b_{n-i}}{b_0}$. We note that we can divide by b_0 since z' is a unit, and we are done.

5

Pick an element $z \in I$ such that $\text{ord}(z) = \min_{w \in I \setminus \{0\}} \{\text{ord}(w)\}$. Then, for any $w \in I \setminus \{0\}$ we have that $z|w$, or equivalently, there exists $r \in \mathbb{Z}_p$ such that $rz = w$. Finally, we note that $\langle z \rangle = \{rz | r \in \mathbb{Z}_p\}$. Clearly $\langle z \rangle \subseteq I$ since I is an ideal, and we also just showed that $I \subseteq \langle z \rangle$, which completes the proof.

6

We prove this by the contrapositive. Say $z_0 := \phi(z) \notin (\mathbb{F}_p^*)^2$. We write $z = \sum_{i \geq 0} a_i p^i$. Assume that $z \in (\mathbb{Z}_p^*)^2$ which implies that $z = y^2$ for some $y \in \mathbb{Z}_p^*$. Say $y = \sum_{i \geq 0} b_i p^i$. Then, $z = y^2 = \sum_{n \geq 0} ((\sum_{i=0}^n b_i b_{n-i}) p^n)$. What is a_0 ? We see that $a_0 = b_0^2$ so that $a_0 \in (\mathbb{F}_p^*)^2$ unless $b_0 = 0$. However, $b = 0$ would imply that $y \notin \mathbb{Z}_p^*$, a contradiction.

7

Assume m is even so that $m = 2r$ for some natural number r . Also assume $z = p^m u$ for some unit $u = (u_n)$ with $u_1 \in (\mathbb{F}_p^*)^2$. We first note that $u := \frac{z}{p^m}$ is a unit. Say we write $u = \sum_{i \geq 0} a_i p^i$.

Now, we wish to construct w such that $z = w^2$. We do so by constructing a w' such that $w'^2 = u$ by induction on n . Then, for our base case we note that $u_1 \in (\mathbb{F}_p^*)^2$. So, there exists w_1 such that $w_1^2 = u_1$. Now, for our inductive step, we assume that we have constructed $w' =: \sum_{i \geq 0} y_i p^i$ so that the first $n-1$ terms of the product w'^2 equal the first n terms of z (when both are thought of as a power series). Namely, we assume that we have chosen y_0, \dots, y_{n-1} so that the coefficients of w'^2 satisfy $\sum_{i=0}^k y_i y_{k-i} = a_k$ for all $k \in [n-1]$. We then wish to choose y_n so that $\sum_{i=0}^n y_i y_{n-i} = a_n$ is satisfied. Well, say $a_n = \sum_{i=0}^n y_i y_{n-i} = 2y_0 y_n + \sum_{i=1}^{n-1} y_i y_{n-i}$. So, we set $y_n := \frac{a_n - \sum_{i=1}^{n-1} y_i y_{n-i}}{2y_0}$. (We note that since y_0 is a unit in \mathbb{F}_p^* we can divide by it). So, now we have inductively constructed w' such that $w'^2 = u$. This gives us $z = p^m w'^2 = (p^r w')^2$ and we are done. Now, for the reverse direction, assume that there exists w such that $w^2 = z$. We wish to show that $\text{ord}_p(z)$ is even and that $z = p^m u$ for some unit u . We consider two cases. Either w is a unit or it is not. Say w is a unit. We write $z = \sum_{i \geq 0} r_i p^i = w^2 = (\sum_{i \geq 0} b_i p^i)^2 = \sum_{n \geq 0} ((\sum_{i=0}^n b_i b_{n-i}) p^n)$ which implies that $r_0 = \sum_{i=0}^0 b_i b_{0-i} = b_0^2 \neq 0$. So, in this case, we get that $\text{ord}_p(z) = 0$ which is even. Additionally, this means that $z = p^0 z$ itself is a unit. Now, what if w is not unit? Then, $\text{ord}_p(w) > 0$. Say $s := \text{ord}_p(w)$. In particular, this means that if we write $w = \sum_{i \geq 0} b_i p^i$, then $b_i = 0$ for $i \in \{0, \dots, s-1\}$ and that $b_s \neq 0$. What does this tell us about the corresponding coefficients in the power series for z ? We note that $z = \sum_{n \geq 0} r_n p^n = w^2 = (\sum_{i \geq 0} b_i p^i)^2 = \sum_{n \geq 0} ((\sum_{i=0}^n b_i b_{n-i}) p^n)$, which means that $r_n = 0$ for all $n \in \{0, \dots, 2s-1\}$ which means that $z_k = \sum_{i=0}^{k-1} r_i p^i = 0$ for all $k \in \{1, \dots, 2s\}$. Now, all that remains to show is that $z_{2s+1} \neq 0$. We note that $z_{2s+1} = \sum_{i=0}^{2s} r_i p^i = 0 + r_{2s} p^{2s} = \sum_{i=0}^{2s} ((\sum_{j=0}^i b_j b_{i-j}) p^i) = (\sum_{j=0}^{2s} b_j b_{2s-j}) p^{2s} = b_s b_s p^{2s}$. So, we get that $z_{2s+1} = (b_s)^2 p^{2s} \neq 0$ and we are done. In particular, we also get in either case that $u := \frac{z}{p^{2s}}$ satisfies $u_1 \neq 0$ which means that u is a unit. That completes the proof.

8

We construct the following isomorphism. In particular, we first construct a homomorphism $\phi : (\mathbb{Q}_p)^* \rightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ as follows. Say we have $w \in (\mathbb{Q}_p)^*$. We know that there exists $u \in (\mathbb{Z}_p)^*$ such that $w = p^m u$ for some $m \in \mathbb{Z}$. Namely, $u = (u_n) = wp^{-m}$ is then a unit in \mathbb{Z}_p . We define $\phi(w) = (0, 0)$ iff m even and $u_1 \in (\mathbb{F}_p^*)^2$. We define $\phi(w) = (1, 0)$ iff m odd and $u_1 \in (\mathbb{F}_p^*)^2$. We define $\phi(w) = (0, 1)$ iff m even and $u_1 \notin (\mathbb{F}_p^*)^2$. We define $\phi(w) = (1, 1)$ iff m odd and $u_1 \notin (\mathbb{F}_p^*)^2$. We then wish to show that such a ϕ defines a group homomorphism under multiplication. Take $w, z \in \mathbb{Q}_p^*$. Say $u = p^{m_1} w$ and $v = p^{m_2} z$ are units in \mathbb{Z}_p . We consider several cases. Case 1: at least one of m_1 or m_2 is even. Case 2: both m_1 and m_2 are odd. We handle case 1. Say WLOG that m_1 is even. So, that $\phi(w) \in \{(0, 0), (0, 1)\}$ or that the projection onto the first component $\pi_1(\phi(w)) = 0$. Then, this means that $m_1 + m_2 = m_2 \pmod{2}$. So, in particular this means that $\pi_1(\phi(wz)) = \pi_1(\phi(z)) = 0 + \pi_1(\phi(z)) = \pi_1(\phi(w)) + \pi_1(\phi(z))$ (because $wz = uv p^{-(m_1+m_2)}$). Now, we consider case 2 in which m_1 and m_2 are odd. In this case, $m_1 + m_2$ is even, which means that $\pi_1(\phi(wz)) = 0 = 1 + 1 = \pi_1(\phi(w)) + \pi_1(\phi(z))$. Now, we consider 2 more cases. Case a: both $u_1, v_1 \in (\mathbb{F}_p^*)^2$. Then, we note that $wz = uv p^{-(m_1+m_2)}$. Also, if we denote $u = \sum_{n \geq 0} r_i p^i$ and $v = \sum_{n \geq 0} s_i p^i$, we note that $uv = \sum_{n \geq 0} ((\sum_{i=0}^n r_i s_{n-i}) p^n)$. In particular, we get that $(uv)_1 = r_0 s_0 = u_1 v_1$ (the way I go back and forth between the power series representation and the infinite product representation gives $u_i = \sum_{l=0}^{i-1} r_l p^l$). So, since there exist $a, b \in (\mathbb{F}_p^*)^2$ such that $u_1 v_1 = a^2 b^2 = (ab)^2$ which means that $(uv)_1 \in (\mathbb{F}_p^*)^2$. So, we get that $\pi_2(\phi(wz)) = 0 = 0 + 0 = \pi_2(\phi(w)) + \pi_2(\phi(z))$. Now, consider the case b in which both $u_1, v_1 \notin (\mathbb{F}_p^*)^2$. As shown in 2 part a, $u_1 v_1 \in (\mathbb{F}_p^*)^2$. So, $\pi_2(\phi(wz)) = 0 = 1 + 1 = \pi_2(\phi(w)) + \pi_2(\phi(z))$. Finally we consider case c in which WLOG $u_1 \in (\mathbb{F}_p^*)^2$ and $v_1 \notin (\mathbb{F}_p^*)^2$. In this case, once again by problem 2 part a, we get that $u_1 v_1 = (uv)_1 \notin (\mathbb{F}_p^*)^2$. So, $\pi_2(\phi(wz)) = 1 = 0 + 1 = \pi_2(\phi(w)) + \pi_2(\phi(z))$. So,

we see that ϕ is a group homomorphism. What is the kernel of ϕ ? It is $w \in \mathbb{Q}_p^*$ where if we have $u = wp^m$ a unit in \mathbb{Z}_p , then m is even, and also that $u_1 \in (\mathbb{F}_p^*)^2$. Now, if $m \leq 0$, then $w = p^{-m}u$ where $-m \geq 0$ and by question 7 we have that $w \in (\mathbb{Z}_p^*)^2 \subseteq (\mathbb{Q}_p^*)^2$. So, assume $m > 0$. Then, note that by question 7, u is a square. So, namely, there exists $c \in \mathbb{Q}_p^*$ such that $c^2 = u = wp^m = wp^{2h}$ which gives $(cp^{-h})^2 = w$ and the result follows.

9

As stated in problem 1. For any field F of characteristic not 2, the quadratic extensions of F are in bijection with the nonidentity elements of $(F^*)/(F^*)^2$. So, we know that there are 3 non identity elements of $(\mathbb{Q}_p^*)/(\mathbb{Q}_p^*)^2$, which means that there are exactly 3 quadratic extensions. We construct these extensions by picking a representative from each of the non-identity classes of $(\mathbb{Q}_p^*)/(\mathbb{Q}_p^*)^2$. The first extension is of the form $\mathbb{Q}_p(p^{-2}u)$ where $u = \sum_{i \geq 0} a_i p^i = a_0$ and $a_0 \notin (\mathbb{F}_p^*)^2$. The second extension is of the form $\mathbb{Q}_p(p^{-1}u)$ where once again $u = \sum_{i \geq 0} a_i p^i = a_0$ with $a_0 \notin (\mathbb{F}_p^*)^2$. The third extension is of the form $\mathbb{Q}_p(p^{-1}u)$ where this time $u = \sum_{i \geq 0} b_i p^i = b_0$ and $b_0 \in (\mathbb{F}_p^*)^2$.