(*October 27, 2005*)

Exercises 5

Paul Garrett garrett@math.umn.edu http://www.math.umn.edu/~garrett/

[5.1] Verify that for a metric $d(,)$ on a space that $\delta(,) = d(,)/[1 + d(,)]$ is also a metric. The issue is the triangle inequality.

[5.2] Prove that $\mathbf{Z}_p \cap \mathbf{Q}$ is the *localization*

$$\mathbf{Z}_{(p)} = \{\frac{a}{b} \in \mathbf{Q} \;:\; a, b \in \mathbf{Z},\; b \neq 0 \bmod p\}$$

of $\mathbf{Z}$ at p (consisting of rational numbers without any factor of p in their denominators).

[5.3] Using the mapping property characterization of the completion of a metric space, show that (as with the presumed inclusion of $\mathbf{Z}_p$ in $\mathbf{Q}_p$) the completion of a subset E of a metric space X has a natural inclusion into the completion of the larger space.

[5.4] Show that an odd integer D has a square root in $\mathbf{Q}_2$ if and only if it has a square root modulo 8.

[5.5] Using the exponential and logarithm functions, show that for a prime $p > 2$ the map

$$p\mathbf{Z}_p \longrightarrow 1 + p\mathbf{Z}_p \subset \mathbf{Z}_p^\times \quad \text{by} \quad x \longrightarrow e^x$$

is an isomorphism of topological groups (with group operation of multiplication in $1 + p\mathbf{Z}_p$).

[5.6] Let $p > 2$ be prime. Show that the quotient group $\mathbf{Q}_p^\times/(\mathbf{Q}_p^\times)^2$ (non-zero p-adic numbers modulo squares) is a group isomorphic to $\mathbf{Z}/2 \oplus \mathbf{Z}/2$, and that, therefore, there are exactly 3 quadratic field extensions of $\mathbf{Q}_p$.

[5.7] Show that there are exactly 7 quadratic field extensions of $\mathbf{Q}_2$.

[5.8] Prove a slightly more complicated version of Hensel's lemma, namely, that for a polynomial f with coefficients in $\mathbf{Q}_p$ and $x_1 \in \mathbf{Q}_p$ such that

$$|f(x_1)|_p < |f'(x_1)|_p^2$$

prove that the recursion $x_{n+1} = x_n - f(x_n)/f'(x_n)$ gives a sequence converging to a root of $f(x) = 0$ in $\mathbf{Q}_p$.

[5.9] Viewing the root-finding version of Hensel's lemma as really just talking about linear factors of polynomials, formulate (and prove correctness of) a similar recursion (and, thereby, *existence* argument) for factoring a polynomial (into possibly higher degree factors) in $\mathbf{Q}_p[x]$ if it factors modulo $p\mathbf{Z}_p$.

[5.10] Determine the factorization of cyclotomic polynomials (defined recursively by)

$$\Phi_n(x) = \prod_{d|n} \frac{x^n - 1}{\Phi_d(x)}$$

(with $\Phi_1(x) = x - 1$) over $\mathbf{Q}_p$. (Consider the case the p does not divide n first.)