Math 296. Homework 6 (due Feb 25)

Book Problems: 1.4: #3, 1.5: #3, 4, 5, 6, 7, 1.6: #5, 6, 9, 2.2 #4, 9

1. Topologies defined by metrics. Let \((X, d)\) be a metric space, that is, a set \(X\) together with a metric \(d\) on it.

   (1) Show that \(X\) has a natural structure of a topological space defined as follows: a set \(U\) is open if for all \(u \in U\) there is a \(\varepsilon\)-ball \(B_\varepsilon(u)\) (with respect to \(d\)) centered at \(u\) which is completely contained in \(U\). By definition, the ball \(B_\varepsilon(u) := \{ x \in X \mid d(x, u) < \varepsilon \}\). (Here, the “ball” \(B_\varepsilon(u)\) is not necessarily “ball shaped” but depends on the metric.) For example, the standard Euclidean topology on \(\mathbb{R}^n\) is the topology defined by the usual Euclidean metric (distance) in \(\mathbb{R}^n\): \(d(x, y) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2}\) where the \(x_i\) are the coordinates of \(x\) and similarly for \(y\).

   (2) Let \(d\) be the metric on \(\mathbb{R}^n\) defined by \(d(x, y) = \max \{|y_i - x_i|\}\), where \(x_i\) denotes the \(i\)-th coordinate of \(x\) and similarly for \(y\). Describe the shape of \(\varepsilon\)-balls in this metric \(n = 1, 2, 3\) and higher.

   (3) Show that the Euclidean metric and the metric in (2) determine the same topology on \(\mathbb{R}^n\).

   (4) Consider two metrics \(d_1\) and \(d_2\) on a set \(X\). For each positive \(\varepsilon\), let \(B^1_\varepsilon(x)\) denote the \(\varepsilon\)-ball with respect to \(d_1\). Show that the two metrics determine the same topology on \(X\) if and only if for each \(x \in X\) and all positive real \(\varepsilon\), there exists \(\delta_\varepsilon\) such that

\[
B^1_\delta(x) \subset B^2_\varepsilon(x) \quad \text{and} \quad B^2_\delta(x) \subset B^1_\varepsilon(x).
\]

2. Compactness in \(\mathbb{R}^n\). A subset \(C\) of \(\mathbb{R}^n\) is said to be bounded if the values of the coordinates of the elements in \(C\) are all bounded. Show that a subset \(X\) of \(\mathbb{R}^n\) is compact if and only if it is closed and bounded. [Hint: this is a good time to make sure you understand the 295 proof in the case \(n = 1\).]

3. Algebraic numbers. Let \(\alpha\) be a complex number. Let \(\mathbb{Q}(\alpha)\) be the intersection of all subfields of \(\mathbb{C}\) containing \(\alpha\).

   (1) Show that \(\mathbb{Q}(\alpha)\) is a field, and the smallest subfield of \(\mathbb{C}\) containing \(\alpha\).

   (2) Show that \(\mathbb{Q}(\alpha)\) is a \(\mathbb{Q}\) vector-space. Is it also a complex vector space? real vector space?

   (3) We say that \(\alpha\) is algebraic if \(\alpha\) satisfies some polynomial with rational coefficients. That is, if there exists rational numbers \(a_i\) such that \(a^n + a_1 a^{n-1} + \cdots + a_{n-1}\alpha + a_n = 0\). Prove that \(\alpha\) is algebraic if and only if the elements \(\{\alpha^i\}_{i \in \mathbb{Z}}\) are linearly dependent.

   (4) Prove that \(\alpha\) is algebraic if and only if \(\mathbb{Q}(\alpha)\) is finite dimensional as a \(\mathbb{Q}\)-vector space.

4. Fields of \(p\) elements. Fix an integer \(n\) greater than 1. Consider the equivalence relation “congruence modulo \(n\)” on \(\mathbb{Z}\). For any integer \(k\), let \(\bar{k}\) denote the equivalence class of \(k\). So, for example, both \(\bar{0}\) and \(\bar{n}\) denote the set of all multiples of \(n\), and \(\bar{1}\) and \(\bar{1} - \bar{17n}\) both denote the set of integers which leave a remainder of 1 when dividing by \(n\). That is,

\[
\bar{i} = \{ i + nk \mid k \in \mathbb{Z} \}.
\]

Let \(\mathbb{Z}_n\) denote the set of these equivalence classes; you proved on an earlier problem set that there are precisely \(n\) equivalence classes in \(\mathbb{Z}\) for this relation, and you thought about “good representatives” of these classes.

   (1) Define a binary operation on \(\mathbb{Z}_n\) as follows:

\[
\mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n
\]

\[
\bar{a} \times \bar{b} \mapsto \bar{a} + \bar{b}.
\]

Show that this is a well-defined (which is to say, independent of the choice of representative for the class), associative, commutative operation with identity, with an inverse for every element. We call this operation “addition” on \(\mathbb{Z}_n\).

   (2) Define a binary operation on \(\mathbb{Z}_n\) as follows:

\[
\mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n
\]

\[
\bar{a} \times \bar{b} \mapsto \bar{a} \bar{b}.
\]
Show that this is a well-defined, associative, commutative operation with identity. We call this operation “multiplication” on $\mathbb{Z}_n$.

(3) Prove that multiplication distributes over addition in $\mathbb{Z}_n$.

(4) Prove that if $n$ is not prime, then there is an element of $\mathbb{Z}_n$ which does not have a multiplicative inverse. Thus this is the only axiom of a field which does not hold in $\mathbb{Z}_n$.\(^1\)

(5) Prove conversely that if $n = p$ is prime, then $\mathbb{Z}_p$ is a field. This is called the “field with $p$ elements”, and often denoted $\mathbb{F}_p$. (Hint: Don’t forget the fundamental theorem of arithmetic.)

(6) Show that every field of $p$ elements is isomorphic to $\mathbb{Z}_p$ for some $p$. (Hint: every field has a multiplicative identity—use this to construct an isomorphism with $\mathbb{F}_p$).

\(^1\)A commutative ring is a set together with two binary operations, called $+$ and $\times$, which are both associative and commutative, and have identity, and such that every element has an inverse with respect to $+$; and multiplication distributes over addition. So you have proved that $\mathbb{Z}_n$ is a commutative ring.