MATH 251: ABSTRACT ALGEBRA I
HOMEWORK #10

Problems (for all)

Problem 1. Show that $(-1)^2 = 1$ in any ring R.

Problem 2. Let $D \in \mathbb{Z}$ be a nonsquare.

(a) Define $\mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D} : a, b \in \mathbb{Q}\} \subset \mathbb{C}$. Show that $\mathbb{Q}(\sqrt{D})$ is a subring of $\mathbb{C}$ (even a subring of $\mathbb{R}$ if $D > 0$).

(b) Show that $\mathbb{Q}(\sqrt{D})$ is a field.

(c) Define $\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} : a, b \in \mathbb{Z}\} \subset \mathbb{Q}(\sqrt{D})$. Show that $\mathbb{Z}[\sqrt{D}]$ is a subring of $\mathbb{Q}(\sqrt{D})$ which is an integral domain but not a field.

(d) Suppose that $D \equiv 1 \pmod 4$. Show that

$$\mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] = \left\{a + b\frac{1+\sqrt{D}}{2} : a, b \in \mathbb{Z}\right\} \subset \mathbb{Q}(\sqrt{D})$$

is a subring of $\mathbb{Q}(\sqrt{D})$. What happens when $D \not\equiv 1 \pmod 4$?

Problem 3. Let $\mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1})$ and similarly $\mathbb{Z}[i]$ be as in Problem 1. Define the map

$$\begin{aligned} N : \mathbb{Q}(i) &\to \mathbb{Q} \\ a + bi &\mapsto (a + bi)(a - bi) = a^2 + b^2. \end{aligned}$$

(a) Show that the restriction $N : \mathbb{Q}(i)^\times \to \mathbb{Q}^\times$ is a homomorphism.

(b) Prove that $a + bi \in \mathbb{Z}[i]$ is a unit if and only if $N(a + bi) = 1$. Conclude that $\mathbb{Z}[i]^\times = \langle i \rangle$. *[Hint: See the text, but only if you are stuck!]*

Problem 4. Show that a division ring has no zerodivisors.

Problem 5. Let F be a field, and let $M_2(F) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in F\right\}$.

(a) Show that $M_2(F)$ is a ring under matrix addition and multiplication. (You may assume that matrix multiplication is associative.)

(b) Show that $M_2(F)$ is not a division ring by exhibiting an explicit zerodivisor.

Problems (for grad students)

Problem 6. Show that there are an *infinite* number of solutions to $x^2 = -1$ in the ring $\mathbb{H}$.

Problem 7. A ring R is called *Boolean* if $a^2 = a$ for all $a \in R$. Show that every Boolean ring is commutative. *[Hint: Not every nonzero element of R is a unit.]*

Date: 14 November 2007; due Wednesday, 28 November 2007.