Math 371 / Problem Set 5 (one page)

More about Rings

Let $R$ be a commutative ring, and $\Sigma \subset R$ be a multiplicative system, i.e., $\Sigma \subset R, \cdot$ is a submonoid. (That is, $1_R \in \Sigma$ and $r, s \in \Sigma \Rightarrow rs \in \Sigma$). Recall that given $\Sigma$, one defines a relation $\sim$ on $R := R \times \Sigma$ by $(a, r) \sim (a', r') \iff \exists s \in \Sigma$ s.t. $ar's = a'r'$.  

1) Prove the assertions mentioned in class:
   
   a) If $\Sigma$ contains no zero divisors, e.g., if $R$ is a domain, then $(a, r) \sim (a', r')$ iff $ar' = a'r$.
   
   b) $\sim$ is an equivalence relation on $R$.

Notation: Denote $\frac{a}{r} := (a, r)/\sim$ and $\Sigma^{-1}R = R/\sim = \{ \frac{a}{r} \mid a \in R, r \in \Sigma \}$.

Define on $R/\sim$ an addition $+$ and multiplication $\cdot$ as follows:

\[
\frac{a}{r} + \frac{b}{s} \overset{\text{def}}{=} \frac{as + br}{rs}, \quad \frac{a}{r} \cdot \frac{b}{s} \overset{\text{def}}{=} \frac{ab}{rs}
\]

2) Prove the assertions from the class:

   a) $+$ and $\cdot$ are well defined (HOW).
   
   b) $R_{\Sigma} := \Sigma^{-1}R, +, \cdot$ is a commutative ring with $0_{R_{\Sigma}} = 0_R/1_R$ and $1_{R_{\Sigma}} = 1_R/1_R$.
   
   c) $\varphi_{\Sigma} : R \to R_{\Sigma}, a \mapsto \frac{a}{1_R}$ is a ring homomorphism.
   
   d) $\varphi_{\Sigma}$ is injective iff $\Sigma$ does not contain any zero divisors.

Terminology: $R_{\Sigma} = \Sigma^{-1}R, +, \cdot$ is the ring of fractions of $R$ with respect to $\Sigma$.

3) Prove/disprove/answer the following:

   a) Let $R = \mathbb{Z}, +, \cdot$ and $\Sigma = \mathbb{Z}\setminus\{0\}$. Then $\Sigma^{-1}\mathbb{Z} = \mathbb{Q}$.
   
   b) Every subring $R \subset \mathbb{Q}$ is of the form $\Sigma^{-1}\mathbb{Z}$ for some $\Sigma$. What the maximal such $\Sigma$?
   
   c) Let $R = R_1 \times R_2$ and $\Sigma = \{(1_{R_1}, a_2) \mid a_2 \in R_2\}$. Describe $\ker(\varphi_{\Sigma}) \subset R$.

4) Prove in all detail the fact that if $R = F[t]$ is the polynomial ring in the variable $t$ over a field $F$, then the division with remainder holds in $R$.

Further, given $p(t) \in R$ of degree $d \geq 0$, give an estimate of the number of operations necessary to divide $f(t) \in R$ by $p(t)$ with remainder in terms of the degree of $f$.

5) Let $\mathbb{Z}[i] \subset \mathbb{C}$ be the ring of Gauss integers. Prove the assertions from the class:

   a) $\varphi : \mathbb{Z}[i] \to \mathbb{N}, a + bi \mapsto a^2 + b^2$ is a Euclidean norm.
   
   b) If $p$ is a prime number, then $p$ is not a prime element of $\mathbb{Z}[i]$ iff $p = n^2 + m^2$ in $\mathbb{N}$.
   
   c) Perform the division with remainder of $20 + 7i$ by $2 + i$.

6) Let $R = \mathbb{Z}[\sqrt{2}] \subset \mathbb{R}$ be as defined in class.

   a) $R$ is a subring of $\mathbb{R}, +, \cdot$ and $\varphi : R \to \mathbb{N}, a + b\sqrt{2} \mapsto |a^2 - 2b^2|$ is a Euclidean norm.
   
   b) Which prime number $p$ are prime elements in $\mathbb{Z}[\sqrt{2}]$?

7) Show that $\varphi : \mathbb{Z}[\sqrt{5}] \to \mathbb{N}, a + b\sqrt{5} \mapsto |a^2 - 5b^2|$ is not a Euclidean norm.

Are there any Euclidean norms on $\mathbb{Z}[\sqrt{5}]$?