Homework set 8 - due 11/05/21

Math 5031

You should solve all the exercises in this assignment, but will only be asked to turn in numbers 1, 2, 3, 6 and 7.

1. Let $R = \mathbb{Z}_{60} \cong \mathbb{Z}/(60)$.
   (a) Show that any ideal in R has the form $(\overline{m})$ where $m|60$.
   (b) Show that if $m|60$, then $\mathbb{Z}_{60}\big/\left(\overline{m}\right) \cong \mathbb{Z}_m$.
   (c) Describe the prime and maximal ideals of R.
2. Show the following:
   (a) $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$.
   (b) $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ are linearly independent over $\mathbb{Q}$.
   (c) $u = \sqrt{2} + \sqrt{3}$ is algebraic over $\mathbb{Q}$ and determine an ideal I such that $\mathbb{Q}[X]/I \cong \mathbb{Q}[u]$.
3. Show that the ideal $I = \left(3, x^3 - x^2 + 2x - 1\right)$ in $\mathbb{Z}[x]$ is not principal.
4. Prove Wilson's theorem: if p is a prime in $\mathbb{Z}$, then we have $(p-1)! \equiv -1 \pmod{p}$. Here's a suggested approach.
   (a) Show that the only elements of $\mathbb{Z}_p$ whose inverses are distinct from themselves are 1 and $p-1$.
   (b) Conclude that the product of the elements in $\mathbb{Z}_p^*$ equals -1.
5. Let R be a commutative ring and S a *multiplicative subset* of R. This means that S is closed under multiplication, $1 \in S$ and $0 \notin S$. Define a relation $\sim$ in $R \times S$ by $(a, s) \sim (b, t)$ if there exists $u \in S$ such that $u(at - bs) = 0$.
   (a) Show that $\sim$ is an equivalence relation.
   (b) Denote the equivalence class of (a, s) as a/s and the set of all the equivalence classes as RS^{-1}. Show that the following operations of addition and multiplication in RS^{-1} are well-defined:

   $$a/s + b/t = (at + bs)/st, \quad (a/s)(b/t) = ab/st, \quad 0 = 0/1, \quad 1 = 1/1.$$

   We call RS^{-1} the *ring of fractions of R by S*. It is also known as the *localization of R by S*. Note: knowing that the elements of RS^{-1} can be added and multiplied just as we do with ratios of integers, checking that it constitutes a (commutative) ring is similar to proving that the rational numbers with the standard operations is a ring. You don't need to prove this here.
   (c) Show that $\varphi : a \mapsto a/1$ is a homomorphism of R into RS^{-1}, and it is a monomorphism (i.e., injective) if and only if no element of S is a zero-divisor in R.
   (d) Show that the elements $s/1$ for all $s \in S$ are units in RS^{-1}.

6. A commutative ring is said to be *local* if it has a unique maximal ideal. Let $R=\mathbb{Z}$, $S=\{b\in\mathbb{Z}: p\nmid b, b\neq 0\}$, and consider the ring of fractions RS^{-1} of R by S. Then RS^{-1} consists of the $a/b\in\mathbb{Q}$ with $p\nmid b$.

   (a) Show that the ideal $(p)=\{a/b : p|a\}$ is maximal in RS^{-1}.

   (b) Prove that RS^{-1} is local.

   (c) If $\mathscr{R}$ is a local ring with the unique maximal ideal $\mathfrak{m}$, prove that $a\in\mathscr{R}$ is a unit if and only if $a\notin\mathfrak{m}$.

7. Let $R=\mathbb{Z}[\sqrt{-10}]$. Find an inverse (fractional ideal) for

$$I=\left(15+25\sqrt{-10},25-40\sqrt{-10}\right)$$

   in R. [Hint: use the Hurwitz's Theorem.]