GROUPS AND RINGS 2021. PROBLEM SHEET 6

QUESTIONS BY ALEXEI N. SKOROBOGATOV

1. Let $d < -1$ be an odd negative integer. Let $R = \mathbb{Z}[\sqrt{d}] = \{m + n\sqrt{d} | m, n \in \mathbb{Z}\}$.

(a) Show that 2 is an irreducible element of R.

(*Hint*: The function $R \to \mathbb{Z}_{\geqslant 0}$ that sends $m+n\sqrt{d}$ to $m^2 - n^2 d$ is multiplicative, i.e., it sends products to products. Hence a factorisation of $m + n\sqrt{d}$ in R gives rise to a factorisation of $m^2 - n^2 d$ in $\mathbb{Z}$.)

(b) Let $a = (1 - d)/2 \in \mathbb{Z}$. Consider the following equality in R:

$$2 \times a = (1 - \sqrt{d}) \times (1 + \sqrt{d})$$

and deduce that R is not a UFD.

2. *Gaussian integers*. Let $R = \mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$, where $i = \sqrt{-1}$. Define

$$\varphi(a + bi) = (a + bi)(a - bi) = a^2 + b^2.$$

(a) Prove that R is an integral domain.

(b) For $r \in R$ show that $r \in R^\times$ if and only if $\varphi(r) = 1$. Compute $R^\times$.

(c) Prove that (R, φ) is a Euclidean domain. (*Hint*: Dividing with remainder in R has something to do with approximating elements of $\mathbb{Q}(i) = \{x + yi | x, y \in \mathbb{Q}\}$ by elements of R.)

(d) Prove that if $\varphi(r)$ is a prime number, then r is an irreducible element of R.

(e) Let $p \in \mathbb{Z}$ be a prime number of the form $3 + 4k$, where $k \in \mathbb{Z}$. Prove that p is an irreducible element of R.

3. *Eisenstein integers*. Let $\zeta = \frac{-1+\sqrt{-3}}{2}$. Let $R = \mathbb{Z}[\zeta] = \{a + b\zeta | a, b \in \mathbb{Z}\}$. Define

$$\varphi(a + b\zeta) = (a + b\zeta)(a + b\bar{\zeta}) = a^2 - ab + b^2.$$

(a) Prove that R is an integral domain.

(b) Compute $R^\times$.

(c) Prove that (R, φ) is a Euclidean domain. (The same hint as in Q2(c).)

(d) Prove that if $\varphi(r)$ is a prime number, then r is an irreducible element of R.

(e) Let $p \in \mathbb{Z}$ be a prime number of the form $2 + 3k$, where $k \in \mathbb{Z}$. Prove that p is an irreducible element of R.

4. Let $\mathbb{H}$ be the division ring of quaternions from Problem Sheet 4, Question 5. Find infinitely many elements $r \in \mathbb{H}$ which satisfy $r^2 + 1 = 0$.

Now, we know that there is a theorem which implies that the polynomial $x^2 + 1 \in k[x]$, where k is a field, has at most 2 roots. Does this contradict the fact that infinitely many elements $r \in \mathbb{H}$ satisfy $r^2 + 1 = 0$?

5. Let R_1 and R_2 be commutative rings. Define the *product* ring $R = R_1 \times R_2 = \{(x, y) | x \in R_1, y \in R_2\}$ by the coordinate-wise addition and multiplication so that $0_R = (0, 0)$ and $1_R = (1, 1)$.

(a) Prove that $R = R_1 \times R_2$ is a ring but never an integral domain.

Date: October 10, 2021.

(b) Show that the projection $R \to R_1$ that forgets the second coordinate is a surjective homomorphism of rings, and similarly for $R \to R_2$.

6. Let R be a commutative ring and let $I, J \subset R$ be ideals in R.

(a) Prove that $I \cap J$ is an ideal in R.

(b) Define $IJ \subset R$ as the set of finite sums $x_1y_1 + \ldots + x_ny_n$, where all $x_i \in I$ and all $y_j \in J$ (for any $n \geqslant 1$). Prove that IJ is an ideal in R.

(c) Prove that $IJ \subset I \cap J$. Give an example when this inclusion is strict.

(d) Consider the map $f\colon R \to (R/I) \times (R/J)$ that sends x to $(x + I, x + J)$. Prove that f is a homomorphism of rings with kernel $I \cap J$.

7. Let R be a commutative ring and let $I, J \subset R$ be ideals in R. Recall from Problem Sheet 4 that $I + J = \{x + y | x \in I, y \in J\}$ is an ideal in R. The ideals I and J are called *coprime* if $I + J = R$.

(a) Prove that if I and J are coprime, then $IJ = I \cap J$.

(b) *Chinese remainder theorem.* If I and J are coprime, then $f\colon R \to (R/I) \times (R/J)$ from Q6(d) gives an isomorphism of rings $R/IJ \cong (R/I) \times (R/J)$.

(c) When $R = \mathbb{Z}$, $I = a\mathbb{Z}$, $J = b\mathbb{Z}$, and $(a, b) = 1$, deduce an isomorphism of rings $\mathbb{Z}/ab\mathbb{Z} \cong \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$.

TODO: add Assessed Coursework.