MATH1050 Examples: Generalizations of divisibility and rationality.

1. We introduce the definition for the notion of *Gaussian integers* below:

   - *Let $z \in \mathbb{C}$. The number z is said to be a* **Gaussian integer** *if both of $\mathsf{Re}(z)$, $\mathsf{Im}(z)$ are integers.*
   - *The set of all Gaussian integers is denoted by $\mathbb{G}$.*

   Prove the statements below:

   (a) *Suppose s is an integer. Then s is a Gaussian integer.*

   (b) *Suppose s is an integer. Then si is a Gaussian integer.*

   (c) *Let s is a Gaussian integer. Suppose $s \neq 0$. Then $|s| \geq 1$.*

   (d) *Suppose s, t are Gaussian integers. Then $\bar{s}$, $s + t$ and st are Gaussian integers.*

   Remark. *Preview* on your *algebra* course. The set $\mathbb{G}$ is a subset of $\mathbb{C}$ and contains $\mathbb{Z}$ as a subset. In your *algebra* course, the set $\mathbb{G}$ is likely denoted by $\mathbb{Z}[i]$. The set $\mathbb{G}$, together with addition and multiplication for complex numbers, constitutes an *integral domain*; further together with the modulus for complex numbers, it constitutes an *Euclidean domain*.

2. *Gaussian integers behave in many ways similar to integers, and similar to polynomials with real coefficients. Many results on the notion of* divisibility *for integers and polynomials with real coefficients in school maths have their analogues for Gaussian integers.*

   We introduce the definition for the notion of *divisibility for Gaussian integers* below:

   - *Let $u, v \in \mathbb{G}$. The number u is said to be* **$\mathbb{G}$-divisible** *by v if there exists some $s \in \mathbb{G}$ such that $u = sv$.*

   Prove the statements below:

   (a) *$25i$ is $\mathbb{G}$-divisible by $3 + 4i$.*

   (b) *0 is $\mathbb{G}$-divisible by 0.*

   (c) *Let $u \in \mathbb{G}$. Suppose u is $\mathbb{G}$-divisible by 0. Then $u = 0$.*

   (d) *Suppose $u \in \mathbb{G}$. Then u is $\mathbb{G}$-divisible by u.*

   (e) *Let $u, v \in \mathbb{G}$. Suppose $u \neq 0$ and u is $\mathbb{G}$-divisible by v. Then $|v| \leq |u|$.*

   (f) *Let $u, v \in \mathbb{G}$. Suppose (u is $\mathbb{G}$-divisible by v and v is $\mathbb{G}$-divisible by u). Then $|u| = |v|$.*

   (g) *Let $u, v, w \in \mathbb{G}$. Suppose (u is $\mathbb{G}$-divisible by v and v is $\mathbb{G}$-divisible by w). Then u is $\mathbb{G}$-divisible by w.*

   (h) *Let $u, v, t \in \mathbb{G}$. Suppose (u is $\mathbb{G}$-divisible by t and v is $\mathbb{G}$-divisible by t). Then $u + v$ is $\mathbb{G}$-divisible by t.*

   (i) *Let $u, v, t \in \mathbb{G}$. Suppose (u is $\mathbb{G}$-divisible by t or v is $\mathbb{G}$-divisible by t). Then uv is $\mathbb{G}$-divisible by t.*

3. *The 'system' of rational numbers is an 'extension' of that of integers. The 'system' of rational functions is an 'extension' of that of polynomials with real coefficients. Here we have an 'extension' of the 'system' of Gaussian integers: it is the 'system' of Gaussian rationals.*

   We introduce the definition for the notion of *Gaussian rationals* below:

   - *Let $z \in \mathbb{C}$. The number z is said to be a* **Gaussian rational** *if there exist some Gaussian integer u, v such that $v \neq 0$ and $u = vz$.*

   Prove the statements below:

   (a) *Suppose z is a rational number. Then z is a Gaussian rational.*

   (b) *Suppose z is a Gaussian integer. Then z is a Gaussian rational.*

   (c) *Suppose $z \in \mathbb{C}$. Then z is a Gaussian rational iff (there exist some $s, t \in \mathbb{Q}$ such that $z = s + ti$.)*

   (d) *Suppose z, w are Gaussian rationals. Then $z + w$ is a Gaussian rational.*

   (e) *Suppose z, w are Gaussian rationals. Then $z - w$ is a Gaussian rational.*

   (f) *Suppose z, w are Gaussian rationals. Then zw is a Gaussian rational.*

   (g) *Suppose z, w are Gaussian rationals. Further suppose $w \neq 0$. Then $\dfrac{z}{w}$ is a Gaussian rational.*

Remark. *Preview* on your *algebra* course. The set of all Gaussian rationals is a subset of $\mathbb{C}$ and contains each of $\mathbb{Q}$ and $\mathbb{G}$ as a subset. In your *algebra* course, it is likely denoted by $\mathbb{Q}[i]$ in some contexts, and by $\mathbb{Q}(i)$ in some other contexts. This set, together with addition and multiplication for complex numbers, constitutes a *field*.

4. *'Division with remainder', as encoded in the statement of the Division Algorithm for Integers, is a phenomenon in the 'system' of integers. It is facilitated by the notion of absolute value, which makes sense of the notion of 'remainder'. In the 'system' of Gaussian integers, there is also a 'Division Algorithm', which is concerned with 'division with remainder'. It is facilitated by the notion of modulus, which makes sense of the notion of 'remainder'.*

   These phenomena make the 'system' of integers, and the 'system' of Gaussian integers, basic examples of algebraic objects known as Euclidean domains.

   (a) Prove the statements below:

      i. *Let $\zeta \in \mathbb{C}$. Suppose $|\zeta| > \frac{1}{\sqrt{2}}$ and $\mathsf{Re}(\zeta) \geq 0$ and $\mathsf{Im}(\zeta) \geq 0$. Then $|\zeta - 1| < |\zeta|$ or $|\zeta - i| < |\zeta|$.*

      ii. *Let $\eta \in \mathbb{C}$. Suppose $|\eta| > \frac{1}{\sqrt{2}}$. Then at least one of $|\eta - 1|$, $|\eta + 1|$, $|\eta - i|$, $|\eta + i|$ is less than $|\eta|$.*

   (b) Prove the **Division Algorithm for Gaussian integers**:

      (♯) *Let $\mu, \nu \in \mathbb{G}$. Suppose $\nu \in \mathbb{G}\backslash\{0\}$. Then there exist some σ, ρ such that $\mu = \sigma\nu + \rho$ and $|\rho| \leq \frac{|\nu|}{\sqrt{2}}$.*

      Hint. Imitate the argument for the Division Algorithm for natural numbers. Apply the Well-ordering Principle for integers to the set $\{x \in \mathbb{N} : \text{There exists some } \kappa \in \mathbb{G} \text{ such that } x = |\mu - \kappa\nu|^2\}$.

      Remark. In the context of the statement (♯), σ and ρ are referred respectively as a quotient and a remainder in the division of the Gaussian integer μ by the Gaussian integer ν. (They are non-unique.)

5. *Gaussian integers are just one amongst many possible generalizations of integers. Here we introduce another generalization.*

   Write $\omega = \frac{1}{2} + \frac{\sqrt{3}}{2}i$. Define the set K by $K = \{z \mid z = a + b\omega \text{ for some } a, b \in \mathbb{Z}\}$.

   Recall that, according to the definition of K:—

   - *Suppose u is a complex number. Then $u \in K$ iff there exist some $c, d \in \mathbb{Z}$ such that $= c + d\omega$.*

   (a) Prove the statements below:

      i. *Suppose $a \in \mathbb{Z}$. Then $a \in K$.*
      ii. *Suppose $b \in \mathbb{Z}$. Then $b\omega \in K$.*
      iii. *Let $z \in K$. Suppose $z \neq 0$. Then $|z|^2$ is a positive integer and $|z| \geq 1$.*
      iv. *Let $z \in K$. Suppose $|z| = 1$. Then $z = \omega^j$ for some j amongst $0, 1, 2, 3, 4, 5$.*
      v. *Suppose $z \in K$. Then $\bar{z} \in K$.*
      vi. *Suppose $z, w \in K$. Then $z + w \in K$.*
      vii. *Suppose $z, w \in K$. Then $zw \in K$.*

   (b) We introduce the definition, called *K-divisibility* below:

      - *Let $u, v \in K$. We say that u is K-**divisible** by v if there exists some $s \in K$ such that $u = sv$.*

      Prove the statements below. Where necessary, you may apply the results stated in the previous part (whether you have proved them or not).

      i. *Suppose $u \in K$. Then u is K-divisible by u.*
      ii. *Let $u, v \in K$. Suppose u is K-divisible by v, and v is K-divisible by u. Then $|u| = |v|$.*
      iii. *Let $u, v, w \in K$. Suppose u is K-divisible by v, and v is K-divisible by w. Then u is K-divisible by w.*
      iv. *Let $u, v \in K$. Suppose $u \neq 0$ and u is divisible by v. Then $|v| \leq |u|$.*
      v. *Let $u, v, z \in K$. Suppose u is K-divisible by z, and v is K-divisible by z. Then $u + v$ is K-divisible by z.*
      vi. *Let $u, v, z \in K$. Suppose u is K-divisible by z, or v is K-divisible by z. Then uv is K-divisible by z.*