MATH 558 EXAM II

Name:

Statements and Definitions.

1. Define integral domain.

Solution. An integral domain is a commutative ring in which $ab = 0$, and $a \neq 0$ implies $b = 0$.

(i) Give an example of an integral domain that is not $\mathbb{Z}$ and not a field.

Solution. The Gaussian integers or a polynomial ring with coefficients in a field are examples of integral domains.

(ii) What conclusion can you draw from the equation $ab = ac$ in the integral domain R assuming $a \neq 0$.

Solution. $b = c$.

(iii) Are the Gaussian integers an integral domain? You must justify your answer.

Solution. The Gaussian integers are an integral domain, because they are contained in a field, namely, the field $\mathbb{C}$.

2. Let R be an integral domain. Define what it means for R to be a Euclidean domain.

Solution. An integral domain R is a Euclidean domain if there exists a function $v : R\backslash 0 \to \{0\} \cup \mathbb{N}$ such that:

(i) $v(a) \leq v(ab)$, for all non-zero $a, b \in R$.

(ii) Given $a, b \in R$, with $b \neq 0$, there exist $q, r \in R$ such that $a = bq + r$, with $r = 0$ or $v(r) < v(b)$.

3. Define greatest common divisor for two elements a, b in a Euclidean domain and state one property you know about the greatest common divisor of a and b.

Solution. In the Euclidean domain R, d is a greatest common divisor of a and b if d divides both a and b and if d' divides a and b then $v(d) \geq v(d')$.

Some properties of GCDs: Let d be a GCD of a and b.

(i) If d' is a common divisor of a and b, then d' divides d.

(ii) There exist $r, s \in R$ such that $d = ra + sb$.

(iii) $v(d)$ is the least element in the set $\{v(ra + sb) \mid r, s \in R \text{ and } ra + sb \neq 0\}$.

4. State the theorem regarding unique factorization in a Euclidean domain.

Solution. Let R be a Euclidean domain and $a \in R$ be a non-zero, non-unit element. Suppose $a = p_1 \cdots p_r$ and $a = q_1 \cdots q_s$, where each p_i, q_j is an irreducible element Then $r = s$, and after (possibly) re-ordering the q_j, $q_1 = u_1 p_1, \ldots, q_r = u_r p_r$, for units $u_1, \ldots, u_r \in R$.

5. Let $F \subseteq K$ be fields. Suppose $\alpha \in K$ is a root of $f(x)$, where $f(x) \in F[x]$ is an irreducible polynomial of degree d. (i) Define $F(a)$ and describe the natural representation of the elements in $F(\alpha)$.

Solution. $F(\alpha)$ is the smallest subfield of K containing F and α. $F(\alpha)$ consists of all elements of K that can be written in the form $a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1}$, with $a_0, \ldots, a_{d-1} \in F$.

(ii) Define what it means for $a(x), b(x) \in F[x]$ to be congruent modulo $f(x)$.

Solution. $a(x)$ is congruent to $b(x)$ mod $f(x)$ if and only if $f(x)$ divides $a(x) - b(x)$.

(iii) Describe the equivalence classes resulting from (ii).

Solution. There is one equivalence for each possible remainder upon division by $f(x)$. In other words, the distinct equivalence classes are all expressions of the form $\overline{a_0 + a_1x + \cdots + a_{d-1}x^{d-1}}$, with $a_0, \ldots, a_{d-1} \in F$.

(iv) In the ring $F[x]$ mod $f(x)$, explain how to multiply two classes from (iii) to get a class of the form you described in (iii).

Solution. $\overline{a(x)} \cdot \overline{b(x)} = \overline{r(x)}$, where $r(x)$ the remainder obtained upon dividing $a(x)b(x)$ by $f(x)$.

Short Answer. 1. Find all of the roots of the polynomial $p(x) = x^3 - x^2 - 4$.

Solution. By the Rational Root test, the possible rational roots of $p(x)$ are: $\pm 1, \pm 2, \pm 4$. Direct calculation shows that $p(2) = 0$, so 2 is one of the roots of $p(x)$. The division algorithm yields: $p(x) = (x-2)(x^2+x+2)$. The quadratic formula yields the other two roots: $\frac{-1 \pm \sqrt{7}i}{2}$.

2. Let $a = 1 + 2i$ and $b = 4 + 6i$ be Gaussian integers. Find Gaussian integers q, r such that $b = aq + r$, with $r = 0$ or $N(r) < N(a)$.

Solution. $4 + 6i = 4 \cdot (1 + 2i) + -2i$. Note: $N(1 + 2i) = 5 > N(-2i) = 4$, so that $r = -2i$ is the remainder when one divides $4 + 6i$ by $1 + 2i$.

Proof Presentation. Let $F \subseteq K$ be fields and $f(x) \in F[x]$ be an irreducible polynomial of degree d. Let $a \in F(\alpha)$ be a non-zero element. Prove that a has a multiplicative inverse of the form $c_0+c_1\alpha+\cdots+c_{d-1}\alpha^{d-1}$.

Solution. Write $a = a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1}$, and set $a(x) = a_0 + a_1x + \cdots + a_{d-1}x^{d-1}$. Since $f(x)$ is irreducible and the degree of $a(x)$ is less than d, the GCD of $a(x)$ and $f(x)$ is 1. Thus, there exist $r_0(x), s(x) \in F[x]$ such that

$$1 = r_0(x)a(x) + s(x)f(x). \qquad (*)$$

If $r_0(x)$ has degree less than d, we substitute $x = \alpha$ to obtain $1 = r_0(\alpha)a(\alpha) + 0 = r_0(\alpha) \cdot a$. Since $r_0(x)$ has degree less than d, $r_0(\alpha) \in F(\alpha)$, and $r_0(\alpha)$ is the multiplicative inverse of a.

If $r_0(x)$ has degree greater than or equal to d, then we write $r_0(x) = q(x)f(x) + r(x)$, with degree $r(x) < d$. Substituting into (*) we obtain,

$$1 = (q(x)f(x) + r(x))a(x) + s(x)f(x) = r(x)a(x) + (q(x)a(x))f(x).$$

Substituting $x = \alpha$ into this last equation, shows that $r(\alpha)$ is the multiplicative inverse of a.