Solutions to Exam 2

Problem 1. a) Define prime and irreducible elements in an integral domain R. (5 points)

b) Let I, J be ideals of a ring R. Define $I + J$ and IJ. (5 points)

c) Define $< a_1, ..., a_k >$, where $a_1, ..., a_k$ are elements of a ring R. Define Noetherian ring. (5 poinst)

d) State the First Isomorphism Theorem (5 points)

e) Define an Euclidean domain. Define unique factorization domain. (6 points)

Solution: A non-zero element $a \in R$ is called **irreducible** if a is non-invertible and whenever $a = xy$ for some $x, y \in R$, either x or y is invertible in R. Equivalently, $a \neq 0$ is irreducible if aR is maximal among all proper principal ideals.

A non-zero element $a \in R$ is called **prime** if a is non-invertible and whenever $a|xy$ then $a|x$ or $a|y$. Equivalently, $a \neq 0$ is prime iff aR is a prime ideal.

b) Let I, J be ideals of a ring R. Then

$$I + J = \{i + j : i \in I,\ j \in J\}.$$

In other words, $x \in I + J$ iff x can be expressed as $i + j$ for some choice of $i \in I$ and $j \in J$.

The ideal IJ is defined as

$$IJ = \{i_1 j_1 + i_2 j_2 + ... + i_m j_m : m \in \mathbb{N},\ i_1, i_2, ..., i_m \in I,\ j_1, ..., j_m \in J\}.$$

Thus, $x \in IJ$ if there is a positive integer m and elements $i_1, i_2, ..., i_m \in I$, $j_1, ..., j_m \in J$ such that $x = i_1 j_1 + i_2 j_2 + ... + i_m j_m$.

c) Let $a_1, ..., a_k$ be elements of a ring R. Then the ideal $< a_1, ..., a_k >$ generated by $a_1, ..., a_k$ is defined as

$$< a_1, ..., a_k >= \{r_1 a_1 + r_2 a_2 + ... + r_k a_k : r_1, r_2, ..., r_k \in R\}.$$

In other words, $x \in < a_1, ..., a_k >$ iff x can be expressed as $r_1 a_1 + r_2 a_2 + ... + r_k a_k$ for some choice of $r_1, r_2, ..., r_k \in R$.

A ring is **Noetherian** if every ideal of R is finitely generated. This means that every ideal of R is of the form $< a_1, ..., a_k >$ for some $k \in \mathbb{N}$ and some elements $a_1, ..., a_k$ in R.

d) **First Isomorphism Theorem:** Let $f : R \longrightarrow S$ be a homomorphism of rings. Set $I = \ker f$. The image $f(R)$ is a subring of S and the map $g : R/I \longrightarrow f(S)$ defined by $g(r + I) = f(r)$ is an isomorphism.

e) An integral domain R is called an **Euclidean domain** if there exists a function $f : R - \{0\} \longrightarrow \{0, 1, 2, 3, ...\}$ such that for any $x, y \in R$, $x \neq 0$ there are $z, r \in R$ such that $y = zx + r$ and either $f(r) < f(x)$ or $r = 0$.

An integral domain R is called a **UFD** (unique factorization domain) if every non-zero, non-invertible element of R can be expressed as a product of irreducible elements and any two such factorizations are equivalent. Two factorizations $x = a_1...a_m = b_1...b_n$ are **equivalent** if $m = n$ and there is a permutation π of the set $\{1, 2, ..., m\}$ such that a_i and $b_{\pi(i)}$ are associated for $i = 1, 2, ..., m$. Two elements a, b of R are **associated** if $a = bu$ for some invertible element u.

Problem 2. a) Define an ideal in a ring R. Define a prime ideal. Define principal ideal. (7 points)

b) Let R be a commutative ring and let $a \in R$. Set $\text{ann}(a) = \{r \in R : ra = 0\}$ (this set is called the **annihilator** of a). Prove that $\text{ann}(a)$ is an ideal in R. (6 points)

c) Let $R = \mathbb{Z}/24$ and let $a = 20$. Find the ideal $\text{ann}(a)$ (it should be of the form $m\mathbb{Z}/24$ for some divisor m of 24). (6 points)

d) Let P be a prime ideal in a commutative ring R. Suppose that $a \in R$ but $a \notin P$. Prove that $\text{ann}(a) \subseteq P$. (6 points)

Solution: a) A non-empty subset I of a ring R is called **ideal** if it has the following two properties:

1. $a - b \in I$ for any $a, b \in R$.

2. $ar \in I$ and $ra \in I$ for any $r \in R$ and any $a \in I$.

A subset I is an ideal iff $I = \ker f$ for some homomorphism $f : R \longrightarrow S$.

An ideal I of a commutative ring R is called **prime** if R/I is a domain. Equivalently, I is prime iff whenever $ab \in I$ for some $a, b \in R$, then either $a \in I$ or $b \in I$.

An ideal I of a commutative ring R is called **principal** if $R =< a >$ (or equivalently, $R = aR$) for some $a \in R$.

b) Suppose that $x, y \in \text{ann}(a)$ and $r \in R$. Then $xa = 0 = ya$. It follows that $(x-y)a = xa - ya = 0$ so $x - y \in \text{ann}(a)$. Furthermore, $(rx)a = r(xa) = r \cdot 0 = 0$, so $rx \in \text{ann}(a)$. This proves that $\text{ann}(a)$ is an ideal.

c) Note that $b \in \text{ann}(20)$ iff $b \cdot 20 = 0$ in the ring $\mathbb{Z}/24$, i.e. iff $24|20b$. This is equivalent to $6|5b$ and also to $6|b$, since $\gcd(5, 6) = 1$. It follows that $\text{ann}(20) = 6\mathbb{Z}/24 = \{0, 6, 12, 18\}$.

d) Let P be a prime ideal of R and suppose that $a \notin P$. If $r \in \text{ann}(a)$ then $ra = 0 \in P$. Since P is prime, either $a \in P$ or $r \in P$. But $a \notin P$, so we must have $r \in P$. This proves that every element of $\text{ann}(a)$ belongs to P, i.e. $\text{ann}(a) \subseteq P$.

Problem 3. a) State the Division Algorithm for polynomials. Explain how does this result imply that polynomial rings over fields are Euclidean domains. (8 points)

b) Find a greatest common divisor of the polynomials $p = x^5 + x^4 + x^3 + x^2 + x + 1$ and $q = x^3 - 1$ in $\mathbb{Q}[x]$. (7 points)

c) Which of the polynomials x^4+4, x^3+x+1, x^2+3 in $\mathbb{F}_5[x]$ are irreducible? Justify your answer. Factor each of these polynomials into irreducible factors. (Here $\mathbb{F}_5$ is the field $\mathbb{Z}/5$). (10 points)

Solution: a) **Division Algorithm.** Let R be a ring and let $f \in R[x]$ be a polynomial whose leading coefficient is invertible. For any polynomial $g \in R[x]$ there are polynomials $h, r \in R[x]$ such that $g = hf + r$ and $\deg r < \deg f$.

If K is a field then every non-zero polynomial has invertible leading coefficient. It follows from the division algorithm that the degree function deg on $K[x] - \{0\}$ makes $K[x]$ an Euclidean domain.

b) Division of p by q yields

$$x^5 + x^4 + x^3 + x^2 + x + 1 = (x^2 + x + 1)(x^3 - 1) + (2x^2 + 2x + 2).$$

Division of $x^3 - 1$ by $2x^2 + 2x + 2$ yields

$$x^3 - 1 = (\frac{1}{2}x - \frac{1}{2})(2x^2 + 2x + 2).$$

Thus $2x^2 + 2x + 2$ is a greatest common divisor of p and q.

Remark. Here is a solution which uses particular features of the polynomials involved. Note that $(x-1)p = x^6 - 1 = (x^3 - 1)(x^3 + 1) = (x - 1)(x^2 + x + 1)(x + 1)(x^2 - x + 1)$. It follows that $p = (x + 1)(x^2 - x + 1)(x^2 + x + 1)$ is an irreducible factorization of p. Irreducible factorization of q is $q = (x - 1)(x^2 + x + 1)$. It is now clear that $x^2 + x + 1$ is a greatest common divisor of p and q. (Note that $x^2 + x + 1$ and $2x^2 + 2x + 2$ are associated so there is no contradiction here.

c) Note that 1 is a root of $x^4 + 4$ (recall that we work over the field $\mathbb{F}_5$). Thus $x + (-1) = x + 4$ is a factor of $x^4 + 4$ and by division we find that $x^4 + 4 = (x + 4)(x^3 + x^2 + x + 1)$. Note that $-1 = 4$ is a root of $x^3 + x^2 + x + 1$. Division algorithm yields $x^3 + x^2 + x + 1 = (x + 1)(x^2 + 1)$. Now 2 is a root of $x^2 + 1$ and $x^2 + 1 = (x + 3)(x + 2)$. We see that $x^4 + 4 = (x + 1)(x + 2)(x + 3)(x + 4)$ is an irreducible factorization.

Remark: Note that $x^4 + 4 = x^4 - 1$ and by Fermat's Little Theorem $1, 2, 3, 4$ are roots of $x^4 - 1$, se we get right away that $x^4 + 4 = (x + 1)(x + 2)(x + 3)(x + 4)$.

By direct verification we se that neither $x^3 + x + 1$ nor $x^2 + 3$ have a root in $\mathbb{F}_5$. It follows that both of these polynomials are irreducible.

Problem 4. a) Let R be PID. Consider two elements $a, b \in R$. Since R is a PID, there is $d \in R$ such that $aR \cap bR = dR$. Prove that for any $c \in R$ we have $d|c$ iff $a|c$ and $b|c$. What would be appropriate name for d? (12 points)

b) Let $R = \mathbb{Z}[\sqrt{6}] = \{a + b\sqrt{6} : a, b \in \mathbb{Z}\}$. Consider the ideal $I =< 2, \sqrt{6} >$. Prove that I and $1 + I$ are different cosets of I in R. Prove that these are the only cosets. What can you say about R/I? (12 points)

Solution: a) Note that $dR \subseteq aR$ and $dR \subseteq bR$ so $a|d$ and $b|d$. Suppose that $d|c$. Then clearly $a|c$ and $b|c$. Conversely, if $a|c$ and $b|c$ then $cR \subseteq aR$ and $cR \subseteq bR$ so $cR \subseteq aR \cap bR = dR$. It follows that $d|c$.

In analogy with the integers, d should be called a least common multiple of a and b.

b) The claim that $I = 0 + I$ and $1 + I$ are different is equivalent to saying that $1 \notin I$. Note that elements of I are of the form $2(a + b\sqrt{6}) + \sqrt{6}(c + d\sqrt{6}) = (2a + 6d) + (2b + c)\sqrt{6}$. None of these elements can be equal to 1 since 1 is odd and $2a + 6d$ is even. Thus indeed $1 \notin I$ and therefore $I \neq 1 + I$.

Let $(a+b\sqrt{6})+I$ be a coset of I. If $a = 2c$ is even then $a+b\sqrt{6} = c \cdot 2+b\sqrt{6} \in I$ so $(a + b\sqrt{6}) + I = I$. If $a = 2c + 1$ is odd then $(a + b\sqrt{6}) - 1 = c \cdot 2 + b\sqrt{6} \in I$ so $(a + b\sqrt{6}) + I = 1 + I$. Thus I and $1 + I$ are the only cosets of I. It follows that $R/I = \{0, 1\}$ is isomorphic to the field $\mathbb{F}_2$ with two elements.

Problem 5. Let $R = \{a + b\sqrt{-2} : a, b \in \mathbb{Z}\}$. Define $N(a + b\sqrt{-2}) = a^2 + 2b^2$ (so N is just the square of the absolute value of the complex number $a + b\sqrt{-2}$. Suppose that $0 \neq x = a + b\sqrt{-2}$ and $y = c + d\sqrt{-2}$ are elements of R. Prove that the complex number y/x can be expressed as $s + t\sqrt{-2}$ for some rational numbers s, t. Use N to prove that R is Euclidean. (10 points)

Solution: a) The first claim follows from the following computation

$$\frac{y}{x} = \frac{c + d\sqrt{-2}}{a + b\sqrt{-2}} = \frac{(c + d\sqrt{-2})(a - b\sqrt{-2})}{(a + b\sqrt{-2})(a - b\sqrt{-2})} = \frac{ac + 2bd + (ad - bc)\sqrt{-2}}{a^2 + 2b^2} =$$

$$= \frac{ac + 2bd}{a^2 + 2b^2} + \frac{ad - bc}{a^2 + 2b^2}\sqrt{-2} = s + t\sqrt{-2},$$

where $s = (ac + 2bd)/(a^2 + 2b^2)$, $t = (ad - bc)/(a^2 + 2b^2)$ are rational numbers.

There are integers k, m such that $|s - k| \leq 1/2$ and $|t - m| \leq 1/2$. Set $p = s - k$ and $q = t - m$. Thus $y/x = (k + l\sqrt{-2}) + (p + q\sqrt{-2})$. In other words,

$$y = (k + l\sqrt{-2})x + (p + q\sqrt{-2})x.$$

Clearly, $k + l\sqrt{-2} \in R$ so $r = (p + q\sqrt{-2})x = y - (k + l\sqrt{-2})x \in R$. Thus $y = (k + l\sqrt{-2})x + r$ and

$$N(r) = N((p + q\sqrt{-2})x) = N(p + q\sqrt{-2})N(x) = (p^2 + 2q^2)N(x).$$

Since $|p| \leq 1/2$ and $|q| \leq 1/2$, we have $p^2 + 2q^2 \leq 1/4 + 2 \cdot (1/4) \leq 3/4$. Thus $N(r) \leq 3N(x)/4 < N(x)$. This shows that N is an Euclidean function on R and R is an Euclidean domain.

Problem 6. Let $R = \mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} : a, b \in \mathbb{Z}\}$ (so this ring is a subring of the Eisenstein integers).

a) Prove that $1, -1$ are the only invertible elements in R. (5 points)

b) Prove that 2, $1 + \sqrt{-3}$, $1 - \sqrt{-3}$ are irreducible in R. Conclude that R is not UFD (find 2 inequivalent factorizations of 4). (5 points)

c) Prove that the ideal $I =< 2, 1 + \sqrt{-3} >$ of R is not principal and that it is maximal. (5 points)

Solution: Define $N(a + b\sqrt{-3}) = a^2 + 3b^2$, so $N(x)$ is just the square of the absolute value of the complex number x. It follows that $N(xy) = N(x)N(y)$.

a) Suppose that $x = a + b\sqrt{-6} \in R$ is invertible. Then $xy = 1$ for some $y \in R$. It follows that $1 = N(1) = N(xy) = N(x)N(y)$. Since $N(x)$ and $N(y)$ are positive integers, we must have $N(x) = 1 = N(y)$. Thus $a^2 + 6b^2 = 1$. Since a, b are integers, we must have $b = 0$ and $a^2 = 1$, i.e. $x = \pm 1$. This shows that 1 and -1 are the only invertible elements of R.

b) Note that if $0 \neq x = a + b\sqrt{-3}$ is not invertible then either $|a| > 1$ or $b \neq 0$. It follows that $N(x) = a^2 + 3b^2 \geq 3$. It follows that if $z \in R$ is not invertible and is not irreducible then $z = xy$ for some non-invertible $x, y \in R$ and $N(z) = N(x)N(y) \geq 3 \cdot 3 = 9$. In other words, if $1 < N(z) < 9$ then z is irreducible. Since $N(2) = 4$, $N(1 + \sqrt{-3}) = 4$ and $N(1 - \sqrt{-3}) = 4$, all three elements 2, $1 + \sqrt{-3}$, $1 - \sqrt{-3}$ are irreducible in R. Note that $4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$. Since $1, -1$ are the only invertible elements of R, no two of the elements 2, $1 + \sqrt{-3}$, $1 - \sqrt{-3}$ are associated and therefore 4 has two inequivalent factorizations into irreducible elements. Thus R is not a UFD.

c) First note that I is a proper ideal. In fact, elements of I are of the form $2(a + b\sqrt{-3}) + (1 + \sqrt{-3})(c + d\sqrt{-3}) = (2a + c - 3d) + (2b + c + d)\sqrt{6}$. If I was not proper, then we would have $1 \in I$ and therefore there would exists integers a, b, c, d such that

$2a+c-3d = 1$ and $2b+c+d = 0$. This would imply that $1 = 1+0 = 2a+2b+2c-2d$ is even, which is clearly false. This shows that I is a proper ideal.

Note now that 2 is irreducible by b). Thus $2R$ is maximal among proper principal ideals of R. Since I is proper and strictly contains $2R$, it can not be principal.

Note that $\mathbb{Z} + I = R$, since $a + b\sqrt{-3} = (a - b) + b(1 + \sqrt{-3} \in \mathbb{Z} + I$ for any $a, b \in \mathbb{Z}$. Now $\mathbb{Z} \cap I$ is a proper ideal of $\mathbb{Z}$ (it is proper since it does not contain 1). Clearly $2 \in \mathbb{Z} \cap I$, so $2\mathbb{Z} \subseteq \mathbb{Z} \cap I$. Since $2\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$ we must have $2\mathbb{Z} = \mathbb{Z} \cap I$. By the third isomorphism theorem, the rings $\mathbb{Z}/2\mathbb{Z}$ and R/I are isomorphic. Since $\mathbb{Z}/2\mathbb{Z}$ is a filed, R/I is a filed too and consequently I is a maximal ideal.