Homework

Frederick Robinson

10 February 2010

Contents

1 Chapter 7 Section 5

1.1 Problem 2

1.1.1 Question

Let R be an integral domain and let D be a nonempty subset of R that is closed under multiplication. Prove that the ring of fractions $D^{-1}R$ is isomorphic to a subring of the quotient field of R (hence is also an integral domain).

1.1.2 Answer

I claim that $D^{-1}R$ is isomorphic to a subring of the quotient field of R, in particular I claim that the subset of the quotient field of R defined by $D^{-1}R$ is itself a subring.

I must therefore demonstrate several properties. Since D is nonempty it contains some r which is in R and therefore $D^{-1}R$ contains the identity in the quotient field of R (just $r^{-1}r = 1$). Moreover, is closed under multiplication since we know that both D^{-1} and R are closed under multiplication. Additionally we have that $D^{-1}R$ is closed under addition since D^{-1} is closed under multiplication (so we can take common denominators) and R is closed under addition.

Since by demonstrating that $D^{-1}R$ contains identity we showed that it is nonempty too we have demonstrated that the subset of the quotient field of

R defined by $D^{-1}R$ is a subring as claimed.

1.2 Problem 4

1.2.1 Question

Prove any subfield of $\mathbb{R}$ must contain $\mathbb{Q}$.

1.2.2 Answer

Let S be a subfield of $\mathbb{R}$. S must contain $1 \neq 0$ since it is a subfield. Moreover in order to be closed under addition it must contain each $n \in \mathbb{N}$ since we can write for each such n, $n = \underbrace{1 + \cdots + 1}_{n \text{ times}}$. Since S is a field, and must therefore be closed under the taking of inverses, it must also contain each inverse, that is $1/n$ for each $n \in \mathbb{N}$. Finally, it must contain each $p/q \in \mathbb{Q}$ by closure under multiplication since such can be expressed in the form $(1/q) \cdot p$. Thus, any subfield of $\mathbb{R}$ must contain $\mathbb{Q}$ as claimed.

2 Chapter 8 Section 1

2.1 Problem 3

2.1.1 Question

Let R be a Euclidean Domain. Let m be the minimum integer in the set of norms of nonzero elements of R. Prove that every nonzero element of R of

norm m is a unit. Deduce that a nonzero element of norm zero (if such an element exists) is a unit.

2.1.2 Answer

Let $x \in R$ such that $N(x) = m$. By the division algorithm $1 = qx + r$ for some $q, r \in R$ with $r = 0$ or $N(r) < N(b)$. Since $N(m)$ is minimal it must be that $r = 0$. So, $1 = qx$ and x is a unit. So, a nonzero element of norm zero must also be a unit since such an element (if it exists) has minimum norm.

2.2 Problem 10

2.2.1 Question

Prove that the quotient ring $\mathbb{Z}[i]/I$ is finite for any nonzero ideal I of $\mathbb{Z}[i]$. [Use the fact that $I = (\alpha)$ for some nonzero α and then use the Division Algorithm in this Euclidean Domain to see that every coset of I is represented by an element of norm less than $N(\alpha)$.]

2.2.2 Answer

Let I be a nonzero ideal of $\mathbb{Z}[i]$. Since $\mathbb{Z}[i]$ is a Principal Ideal Domain we can write $I = (\alpha)$ for some $\alpha \neq 0$. Moreover, since $\mathbb{Z}[i]$ is a Euclidean Domain, given an arbitrary $x \in \mathbb{Z}[i]$ we can write $x = \alpha q + r$ for some r with $N(r) < N(\alpha)$ or $r = 0$. Since there are but a finite number of such r there are but a finite number of cosets of (α) in $\mathbb{Z}[i]$ as claimed.

3 Chapter 8 Section 2

3.1 Problem 3

3.1.1 Question

Prove that a quotient of a P.I.D. by a prime ideal is again a P.I.D.

3.1.2 Answer

Let P be a Principal Ideal Domain, and Q be a prime ideal in P. We seek to prove that P/Q is a Principal Ideal Domain. If Q is the zero ideal then P/Q must be a Principal Ideal Domain since it is just isomorphic to P which is itself a Principal Ideal Domain.

If however, Q is nonzero then Q is maximal in P by Proposition 7. Let L be an ideal in P/Q. Then the preimage $M = \varphi^{-1}(L)$ of L under the natural ring homomorphism $\varphi : P \to P/Q$ is an ideal in P. Then since Q is a maximal ideal in P a P.I.D. there are two cases. Either $M \subseteq Q$ in which case $L = (1)$ or $P = QM$ (if neither of these is the case then the Q is not maximal as it is contained in QM). If $P = QM$ then each $p \in P$ can be written as $qm = p$ for some $q \in Q$ and $m \in M$. Applying the homomorphism property this implies that $\varphi(q)\varphi(m) = \varphi(p)$ and since each element of P/Q can be written as $\varphi(p)$ for some p and $\varphi(q) = 1$ it must be that $\varphi(M) = L = P/Q$. So in this case too, L is Principal as in particular $(\overline{1}) = L$.

So we have established that a quotient of a P.I.D. by a prime ideal is

again a P.I.D as desired.

3.2 Problem 4

3.2.1 Question

Let R be an integral domain. Prove that if the following two conditions hold then R is a Principle Ideal Domain.

1. any two nonzero elements a and b in R have a greatest common divisor which can be written in the form $ra + sb$ for some $r, s \in R$, and

2. if $a_1, a_2, a_3, \ldots$ are nonzero elements of R such that $a_{i+1}|a_i$ for all i, then there is a positive integer N such that a_n is a unit times a_N for all $n \geq N$.

3.2.2 Answer

Suppose that $I \subset R$ is an ideal in R. Call its elements $I = \{i_1, i_2, \ldots\}$. Then construct a sequence $G = \{g_1, g_2, \ldots\}$ from I in the following manner.

$$g_j = \begin{cases} \gcd(i_1, i_2) & j = 1 \\ \gcd(i_{j+1}, g_{j-1}) & \text{otherwise} \end{cases}$$

By Property 1 this sequence G must exist, and be a subset of the ideal I since an element of the form $ra + sb$ for $a, b \in I$ must also be in I. Moreover, the element g_N whose existence is ensured by Property 2 must generate the

ideal I. It divides every element i_n for $n < N$ since it divides a divisor of each such element (namely g_n). It also divides every i_n with $n > N$ since it is an associate of a divisor of each such i_n by Property 2.

So we have demonstrated a generator for an arbitrary ideal I in R. Hence, I is a Principal Ideal Domain.

3.3 Problem 5

3.3.1 Question

Let R be the quadratic integer ring $\mathbb{Z}[\sqrt{-5}]$. Define the ideals $I_2 = (2, 1 + \sqrt{-5}), I_3 = (3, 2 + \sqrt{-5})$, and $I_3' = (3, 2 - \sqrt{-5})$.

1. Prove that I_2, I_3, and I_3' are nonprincipal ideals in R. [Note that Example 2 following Proposition 1 proves this for I_3.]

2. Prove that the product of two nonprincipal ideals can be principal by showing that $I_2^2 = (2)$.

3. Prove similarly that $I_2 I_3 = (1 - \sqrt{-5})$ and $I_2 I_3' = (1 + \sqrt{-5})$ are principal. Conclude that the principal ideal (6) is the product of 4 ideals: $(6) = I_2^2 I_3 I_3'$.

3.3.2 Answer

1. As this statement is proven in the book for for I_3 we will prove it only for I_2 and I_3'.

Let N be the norm associated with the quadratic integer ring $\mathbb{Z}[\sqrt{-5}]$ defined by $N(a+b\sqrt{-5}) = a^2+5b^2$. Suppose that I_2 were principal. Then there would be some $a+b\sqrt{-5}$ so that $a+b\sqrt{-5}$ generates I_2. In particular we would have $2 = \alpha(a+b\sqrt{-5})$ and $1+\sqrt{-5} = \beta(a+b\sqrt{-5})$ for some $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$.

Norming each of these we see that we would need $4 = N(\alpha)(a^2+5b^2)$ and $6 = N(\beta)(a^2+5b^2)$. However this would necessitate by the first equation $b = 0$, and $a = 1$ or $a = 2$. Taking the second into account we would need $a = 1$ since there is no integer $N(\beta)$ that would give $N(\beta)\cdot 4 = 6$. However, if $a = 1$ and $b = 0$ this would just be the generator for the entire ring, and I_2 is not the entire ring since it does not contain 1.

Similarly for I_3' assuming the existence of a generator $a+b\sqrt{-5}$ implies that $9 = N(\alpha)(a^2+5b^2)$ and $9 = N(\beta)(a^2+5b^2)$. Then, it is easy to check that the only options for generators are the ones which are listed already. However, now we can see that there can be no single generator for the entire ideal as there are elements of I_3' which are generated by one of the generators but not the other. In particular $3 \notin (2-\sqrt{-5})$ and $3-\sqrt{-5} \notin (3)$.

2. Each element of I_2^2 is of the form $a(2)b(1+\sqrt{-5})$ or $a(2)b(2)$ or $a(1+\sqrt{-5})b(1+\sqrt{-5})$. It should be clear that the elements of the first forms are members of (2). We check elements of the last form. Expanding we

see that they can be written as $-14(ab)$ and are thus members of (2). Hence each element of I_2^2 is a member of (2) as claimed. Since each element of (2) is in the squared ring.

3. Elements of $I_2 I_3$ can be written as products of the form $a(3)(2)$ or $(2)(2+\sqrt{-5})(a)$ or $(1+\sqrt{-5})(3)(a)$ or $a(1+\sqrt{-5})(2+\sqrt{-5})$. Since these forms can be expanded as $(6)a$, $(4+2\sqrt{-5})a$, $(3+3\sqrt{-5})a$, and $(-3+3\sqrt{-5})a$ respectively $I_2 I_3 = (1+\sqrt{-5})$ as claimed. We can show a simlar statement for $I_2 I_3'$ and so it follows that $(6) = I_2^2 I_3 I_3'$