412 Individual HW4

Jack Madden

March 2024

Problem 1

a) If K is an ideal in R/I, then K must contain I as K is an additive subgroup of R/I and $0 + I = I$ is the additive identity. Thus, $I \in \pi^{-1}(K)$. We then show that $\pi^{-1}(K)$ is an ideal in R. We have that $\pi^{-1}(K)$ is an additive subgroup in R as subgroups correspond to subgroups under homomorphism and K is an additive subgroup as that is a condition of being an ideal. Then, suppose $r \in R$, $k \in \pi^{-1}(K)$. Then $\pi(rk) = \pi(r)\pi(k)$. Since $\pi(k) \in K$, $\pi(r)\pi(k) = \pi(rk) \in K$ and therefore $r\pi^{-1}(K) \subseteq \pi^{-1}(K)$ for any $r \in R$ and thus $\pi^{-1}(K)$ is an ideal.

b) We must show that $\pi(J)$ is an ideal in R/I. $\pi(J)$ is an additive subgroup of R/I. Thus it is sufficient to show that for any $r \in R$, $\pi(r)\pi(J)$ is in $\pi(J)$. $\pi(r)\pi(J) = \pi(rJ)$. Since rJ is a subset of J, its image under π will be a subset of J. Thus, any ideal J containing I can be written as $\pi^{-1}(K)$ for $K = \pi(J)$.

c) We have that this map is injective, take K, L ideals in R/I, as if $\pi^{-1}(K) = \pi^{-1}(L)$, $\pi(\pi^{-1}(K)) = \pi(\pi^{-1}(L)) \to K = L$. We have the surjectivity of this map from part (b).

Problem 2

Clearly, $\sim$ is reflexive, as $a = 1 \cdot a$ and 1 is a unit. Also, if $a = ub$, then $b = u^{-1}a$, and we know u^{-1} exists as u is a unit, and thus $\sim$ is symmetric. Also, suppose $a = ub$, $b = u'c$. Then $a = uu'c$, and uu' is a unit having inverse $u'^{-1}u^{-1}$. Thus $\sim$ is transitive and therefore an equivalence relation.

Problem 3

This bijection is to send any principal ideal (n) to the equivalence class with representative n. We first show that this map is injective. Suppose $n \sim m$. Then $(n) = rn \; \forall r \in R$, and $(m) = rm \; \forall r \in R$. But we have $m = un$ for some unit u in R. So $(m) = r(un)$. Let us show that these sets are equal. Clearly for any $ru(n) \in (m)$, $ru = r' \in R$ and $r'n \in (n)$, so $(m) \subseteq (n)$. Also, take any $rn \in (n)$. Let $r' = ru^{-1}$, then $r'(un) = rn \in (m)$. So $(n) \subseteq (m)$ and therefore $(m) = (n)$. Thus $m \sim n \to (m) = (n)$. Map is also clearly surjective as if we take some representative of an equivalence class n, it is an element in R and thus inherently generates some principal ideal.

Problem 4

Suppose that f can be written as $g(x)h(x)$ for $deg(g) = m, deg(h) = n < deg(f), m \leq n$. Let $g(x) = a_m x^m + \cdots + a_0$, $h(x) = b_n x^n + \cdots + b_0, f(x) = c_{m+n}x^{m+n} + \cdots + c_0$. We have that the constant coefficient in $f(x)$ is $a_0 b_0$. We know that p may only be in the factorization of either a_0 or b_0. Choose $p \mid a_0$. By strong induction, we will show that $p \mid a_i \forall i \leq m$. Suppose $p \mid a_j, \forall j \leq i-1$. Then,

$$c_i = a_i b_0 + a_{i-1}b_1 + \cdots + a_0 b_i$$

By our inductive hypothesis we have that:

$$c_i = a_i b_0 + pr$$

for some $r \in R$ Also, since $i \le m < m+1 \le m+n$, $p \mid c_i$: Therefore, for some $r' \in R$,

$$a_i b_0 = p(r - r')$$

Since $p \nmid b_0$, $p \mid a_i$ Therefore, we can conclude that $p \mid a_m$ and therefore $p \mid a_m b_n$. However, we also have $p \nmid a_m b_n$. This implies that $a_m b_n$ admits two non-associative factorizations which cannot be true in a UFD. Therefore, contradiction.

Problem 5

We can think of this polynomial as being in the ring of polynomials with coefficients in $\mathbb{C}[y]$. Since $\mathbb{C}$ is a field, and therefore a UFD, $\mathbb{C}[y]$ is a UFD, and then $(\mathbb{C}[y])[x]$ is a UFD by the same logic. Thus we can apply the more general criterion proved in Problem 4. We have coefficients $a_7 = 1, a_0 = (y^2-1)$. $y^2 - 1 = (y+1)(y-1)$, so $(y+1) \mid (y^2-1)$ but $(y+1)^2 \nmid (y^2-1)$ and $(y+1) \nmid 1 = a_7$. $(y+1)$ is clearly irreducible as it is linear. Thus, this polynomial is irreducible.

Problem 6

We show that this is an ideal. First we show that it is an additive subgroup. We have that $0 = 0r_1 + 0r_2 + \cdots + 0r_s \in (r_1, \dots, r_s)$. Also, suppose $c = a_1r_1 + a_2r_2 + \cdots + a_sr_s \in (r_1, \dots, r_s)$. Also, $d = -a_1r_1 + -a_2r_2 + \cdots + -a_sr_s \in (r_1, \dots, r_s)$. $c + d = r_1(a_1 - a_1) + \cdots + r_s(a_s - a_s) = r_1 0 + \cdots + r_s 0 = 0$ by distributivity thus $d = -c \in (r_1, \dots, r_s)$ and therefore $(r_1, \dots, r_s)$ contains inverses. Also, suppose $a = a_1r_1 + a_2r_2 + \cdots + a_sr_s$, $b = b_1r_1 + b_2r_2 + \cdots + b_sr_s$. By distributivity, $a + b = (a_1 + b_1)r_1 + \cdots + (a_s + b_s)r_s \in (r_1, \dots, r_s)$. Thus, $(r_1, \dots, r_s)$ is an additive subgroup. Also, let $r \in R$. Then for any $a_1r_1 + \cdots + a_sr_s \in (r_1, \dots, r_s)$, $r(a_1r_1 + \cdots + a_sr_s) = (ra_1)r_1 + \cdots + (ra_s)r_s \in (r_1, \dots, r_s)$. Thus it is an ideal.

Problem 7

Suppose that $I(f) \neq R$. In this case, $I(f)$ must be contained in some maximal ideal $M \neq R$. Consider then the ring of polynomials $R/M[x]$. We know that since R/M is a field, $R/M[x]$ must be at least an integral domain. We also have that $g(x)$ and $h(x)$ cannot be zero in this integral domain for the following reason. Let $g(x) = a_m x^m + \cdots + a_0, h(x) = b_n x^n + \cdots + b_0, f(x) = c_{m+n}x^{m+n} + \cdots + c_0$. If $g(x), h(x)$ are zero in this domain, then all of their coefficients are in $I(f)$. If this is the case, then for $g(x)$ (and therefore also $h(x)$,

$$g(x) = (a_{n+m}r_{n+m} + \cdots + a_0r_0)x^m + \cdots + (a_{n+m}s_{n+m} + \cdots + a_0s_0)$$

where $r_i, s_i \in R$. Linear combinations of these coefficients are then:

$$t_m(a_{n+m}r_{n+m} + \cdots + a_0r_0) + \cdots + t_0(a_{n+m}s_{n+m} + \cdots + a_0s_0)$$

which by distributivity is:

$$(a_{n+m}t_mr_{n+m} + \cdots + a_0t_mr_0) + \cdots + (a_{n+m}t_0s_{n+m} + \cdots + a_0t_0s_0)$$

$$a_{n+m}(t_mr_{n+m} + \cdots + t_0s_{n+m}) + \cdots + a_0(t_mr_0 + \cdots t_0s_0)$$

which then implies that $I(g) \subseteq I(f) \neq R$ which cannot be the case. So we have that $f(x), g(x) \neq 0 \in R/M[x]$, but $f(x)g(x) = 0 \in R/M[x]$, as all the coefficients of $f(x)g(x)$ are clearly linear combinations of coefficients of $f(x)g(x)$. This is a contradiction as $R/M[x]$ is an integral domain.

Problem 8

a) We have that $(x+1)^2 + (x+1) + 1 = (x^2+1+x+1+1) = x^2+x+1$ which is in $0 + (x^2+x+1)$ in the quotient ring. Also, x^2+x+1 is in $0+(x^2+x+1)$ in the quotient ring. So $\alpha = (x+1)+I, x+I$.

b) We have that x^2+x+1 has roots at α. Since it is a quadratic, these roots are its factors. Choose $\alpha = x$. Then $x^2+x+1 = (x+\alpha)(x+(\alpha+1)$.

Problem 9

We have that this polynomial is irreducible as it has no roots and is cubic, $f(0) = 1, f(1) = \alpha, f(\alpha) = \alpha+1, f(\alpha+1) = \alpha$.

Problem 10

a) Since $x^2-\alpha$ is a quadratic, it is sufficient to show that if there exists an α such that $x^2-\alpha$ has no roots, $x^2-\alpha$ is irreducible. The roots of $x^2-\alpha$ must satisfy the equation $x^2=\alpha$. We know that the set $x^2|x \in \mathbb{Z}_p$ can have size at most $p-1$, as both $1^2 = 1$ and $(p-1)^2 = 1$. Thus, there exists some α such that there is no x such that $x^2 = \alpha$ and thus there exists some α such that $x^2-\alpha$ is irreducible.

b) Since $x^2-\alpha$ is irreducible, and therefore the ideal generated by it is maximal, the quotient ring $\mathbb{Z}_p/(x^2-\alpha)$ is a field. It has p^2 elements as its elements are the remainders of polynomial division by $x^2-\alpha$ which are $nx+m$, where $n \in [0, p-1](p \text{ choices}), m \in [0, p-1](p \text{ choices})$.

Problem 11

a) Let us show that this is a subring of $K[x]$. We have that it is an additive subgroup by the fact that the zero polynomial has $a_1 = 0$, also, if we have $a_0 + a_2x^2 + a_3x^3 + \cdots + a_nx^n \in R$, then $-a_0 + -a_2x^2 + -a_3x^3 + \cdots - a_nx^n \in R$. Also, by distributivity,

$$(a_0+a_2x^2+\cdots+a_nx^n+b_0+b_2x^2+\cdots b_mx^m) = (a_0+b_0)+(a_2+b_2)x^2+\cdots+(a_m+b_m)x^m+\cdots a^nx^n \in R$$

. Also, since the coefficient of the linear term of the multiplication of two polynomials is equal to $a_1b_0 + b_1a_0$, and $a_1, b_1 = 0$, the linear term of the multiplication of two polynomials in R will also be in R. So it is is a subring.

b) As a counterexample, if we choose $K = \mathbb{C}$, we see that the polynomial $x^4 - 2 \in R \subset \mathbb{C}[x]$ has the two factorizations in R, $(x^2-\sqrt{2})(x^2+\sqrt{2}), (x^2+\sqrt{2}i)^2$.