MATH 5590H HOMEWORK 12

BRENDAN WHITAKER

Exercise 7.6.7. *Let $n|m$, $n,m \in \mathbb{N}$. Prove that the natural surjective ring projection $\pi : \mathbb{Z}_m \to \mathbb{Z}_n$ is also surjective on the units: $\mathbb{Z}_m^\times \to \mathbb{Z}_n^\times$.*

Proof. Let $n|m$, $n,m \in \mathbb{N}$. By corollary 18 and the Chinese remainder theorem, we know that if $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, $m = p_1^{\beta_1} \cdots p_k^{\beta_k}$, where $\beta_i \leq \alpha_i$ $\forall i$, then

$$\begin{aligned} \mathbb{Z}_m &= \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}}, \\ \mathbb{Z}_n &= \mathbb{Z}_{p_1^{\beta_1}} \times \cdots \times \mathbb{Z}_{p_k^{\beta_k}}, \\ \mathbb{Z}_m^\times &= \mathbb{Z}_{p_1^{\alpha_1}}^\times \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}}^\times, \\ \mathbb{Z}_n^\times &= \mathbb{Z}_{p_1^{\beta_1}}^\times \times \cdots \times \mathbb{Z}_{p_k^{\beta_k}}^\times. \end{aligned} \tag{1}$$

So if $\pi : \mathbb{Z}_m \to \mathbb{Z}_n$ is the natural projection homomorphism, we know π is surjective, and $\pi_i : \mathbb{Z}_{p_i^{\alpha_i}} \to \mathbb{Z}_{p_i^{\beta_i}}$ is also surjective. We want to show $\pi_i : \mathbb{Z}_{p_i^{\alpha_i}}^\times \to \mathbb{Z}_{p_i^{\beta_i}}^\times$ is surjective. Let $x_i \in \mathbb{Z}_{p_i^{\beta_i}}^\times$. Then we must have that $(x_i, p_i) = 1$. And $\pi_i^{-1}(x_i) = \{l_i p_i^{\beta_i} + x_i : 0 \leq l_i \leq p_i^{\alpha_i - \beta_i} - 1, l_i \in \mathbb{Z}\}$. Suppose $(l_i p_i^{\beta_i} + x_i, p_i^{\alpha_i}) = a_i > 1$ $\forall l_i$. We know if $a_i | l_i p_i^{\beta_i}$, and $a_i | p_i^{\alpha_i}$, then $a_i = p_i^{\gamma_i}$ for some non-negative integer $\gamma_i \leq \alpha_i$. Let $l_i = 1$. Then $(p_i^{\beta_i} + x_i, p_i^{\alpha_i}) = p_i^{\gamma_i}$. So $\exists r_i \in \mathbb{Z}$ s.t. $p_i^{\beta_i} + x_i = r_i p_i^{\gamma_i} \Rightarrow x_i = r_i p_i^{\gamma_i} - p_i^{\beta_i}$. We assume $\beta_i > 0$ else $\mathbb{Z}_{p_i^{\beta_i}} = 1$, and π_i is the trivial homomorphism, hence surjective on the units. And $\gamma_i > 0$, else $a_i = 1$, so $p_i | x_i$, which is a contradiction since we said $(x_i, p_i) = 1$, so we must have that $a_i = p_i^{\gamma_i} = 1$ $\forall i$, so $(p_i^{\beta_i} + x_i, p_i^{\alpha_i}) = 1$ $\forall i$, so $\exists y_i = x_i + p_i^{\beta_i} \in \mathbb{Z}_{p_i^{\alpha_i}}^\times$ s.t. $\pi_i(y_i) = x_i$, so $\pi_i : \mathbb{Z}_{p_i^{\alpha_i}}^\times \to \mathbb{Z}_{p_i^{\beta_i}}^\times$ is surjective on the units, hence $\pi : \mathbb{Z}_m^\times \to \mathbb{Z}_n^\times$ is surjective on the units. □

Exercise 8.3.3. *Determine all the representations of the integer $2130797 = 17^2 \cdot 73 \cdot 101$ as a sum of two squares.*

We first find all the representations of $73 \cdot 101 = 7373$. Now $73 = (8+3i)(8-3i)$ and $101 = (10+i)(10-i)$, so if we wish to write $7373 = A^2 + B^2$, the possible factorizations of $A + Bi$ in the Gaussian integers are

$$\begin{aligned} (8+3i)(10+i) &= 80 + 38i - 3 = 77 + 38i, \\ (8+3i)(10-i) &= 80 + 22i + 3 = 83 + 22i, \\ (8-3i)(10+i) &= 80 - 22i + 3 = 83 - 22i, \\ (8-3i)(10-i) &= 80 - 38i - 3 = 77 - 38i. \end{aligned} \tag{2}$$

Then $7373 = (\pm 77)^2 + (\pm 38)^2 = (\pm 83)^2 + (\pm 22)^2$, which gives us 8 possible combinations, and switching the order of A and B gives us another 8, for a total of 16 representations. So by multiplying each of A and B by 17, we get 16 unique representations of 2130797 as a sum of two squares of the form $(17A)^2 + (17B)^2$. But since $17 \equiv 1 \mod 4$, we have additional representations. Note that $17^2 = (4+i)^2(4-i)^2$. Thus we have

Date: AU17.

several factorizations if $A = Bi$ s.t. $A^2 + B^2 = 2130797$ given by:

$$\begin{aligned}
(4+i)^2(8+3i)(10+i) &= 851 + 1186i,\\
(4+i)^2(8+3i)(10-i) &= 1069 + 994i,\\
(4+i)^2(8-3i)(10+i) &= 1421 + 334i,\\
(4+i)^2(8-3i)(10-i) &= 1459 + 46i,\\
(4-i)^2(8+3i)(10+i) &= 1459 - 46i,\\
(4-i)^2(8+3i)(10-i) &= 1421 - 334i,\\
(4-i)^2(8-3i)(10+i) &= 1069 - 994i,\\
(4-i)^2(8-3i)(10-i) &= 851 - 1186i.
\end{aligned} \tag{3}$$

So we have $2130797 = (\pm 851)^2 + (\pm 1186)^2 = (\pm 1069)^2 + (\pm 994)^2 = (\pm 1421)^2 + (\pm 334)^2 = (\pm 1459)^2 + (\pm 46)^2$. This gives us 16 combinations, and switching the order of A and B gives us another 16, so we have 32 additional representations of 2130797 as a sum of two squares, for a total of 48.

Exercise 8.3.6.

(a) *Prove that the quotient ring $Q = \mathbb{Z}[i]/(1+i)$ is a field of order 2.*

Proof. Observe:

$$\mathbb{Z}[i]/(1+i) \cong \mathbb{Z}[x]/(x^2+1, x+1) \cong \mathbb{Z}[-1]/((-1)^2+1) = \mathbb{Z}/(2) \cong \mathbb{Z}_2. \tag{4}$$

□

(b) *Let $q \in \mathbb{Z}$ be a prime with $q \equiv 3 \mod 4$. Prove that the quotient ring $\mathbb{Z}[i]/(q)$ is a field with q^2 elements.*

Proof. Note since $q \equiv 3 \mod 4$, we know q is irreducible, and since the Gaussian integers are a UFD, we know q is also prime by Proposition 8.3.18. Then we must have that (q) is a prime ideal. Since $\mathbb{Z}[i]$ is also a principal ideal domain, we know that (q) is also a maximal ideal by Proposition 8.2.7, which means $\mathbb{Z}[i]/(q)$ is a field since $\mathbb{Z}[i]$ is commutative, by Proposition 7.4.12. Then since $1, i$ generate $\mathbb{Z}[i]$, they also generate $\mathbb{Z}[i]/(q)$, so we have two cyclic subgroups $\langle 1\rangle, \langle i\rangle$, each of order q. Now $\mathbb{Z}[i]/(q) = \langle 1\rangle + \langle i\rangle$ and $\langle 1\rangle \cap \langle i\rangle = 0$ so we must have that $\mathbb{Z}[i]/(q) \cong \langle 1\rangle \times \langle i\rangle \cong \mathbb{Z}_q^2$ as groups. Thus our field must have q^2 elements. □

(c) *Let $p = \pi\overline{\pi} \equiv 1 \mod 4$ be a prime in $\mathbb{Z}$. Show that the hypotheses for the Chinese remainder theorem are satisfied, and that $\mathbb{Z}[i]/(p) \cong \mathbb{Z}[i]/(\pi) \times \mathbb{Z}[i]/(\overline{\pi})$ as rings. Show that the quotient ring $\mathbb{Z}[i]/(p)$ has order p^2 and conclude that $\mathbb{Z}[i]/(\pi)$ and $\mathbb{Z}[i]/(\overline{\pi})$ are both fields of order p.*

Proof. By Proposition 8.3.18, we know that p can be written as a sum of two squares, so $p = a^2 + b^2 = (a+bi)(a-bi) = \pi\overline{\pi}$. And by the same Proposition, we know $\pi, \overline{\pi}$ are irreducibles in $\mathbb{Z}[i]$, and since we are in a UFD, we know these elements are also prime. Then we know that they are coprime and so since $\mathbb{Z}[i]$ is a Euclidean domain, we know $\exists r, s \in \mathbb{Z}[i]$ s.t. $r\pi + s\overline{\pi} = 1$, so since $(1) = \mathbb{Z}[i]$, we know that $(\pi) + (\overline{\pi}) = \mathbb{Z}[i]$, and hence they are comaximal ideals, and thus the hypotheses for the Chinese remainder theorem are satisfied. Then from this, we know $(\pi) \cap (\overline{\pi}) = (\pi)(\overline{\pi}) = (p)$. Hence we have $\mathbb{Z}[i]/(p) = \mathbb{Z}[i]/((\pi) \cap (\overline{\pi})) \cong \mathbb{Z}[i]/(\pi) \times \mathbb{Z}[i]/(\overline{\pi})$ as rings. Then since $\mathbb{Z}[i]$ is also a PID, we know $(\pi), (\overline{\pi})$ are maximal ideals, and thus $\mathbb{Z}[i]/(\pi), \mathbb{Z}[i]/(\overline{\pi})$ are fields since $\mathbb{Z}[i]$ is commutative. Finally, $\mathbb{Z}[i]/(p) \cong \mathbb{Z}_p[i] = \{a + bi : a, b \in \mathbb{Z}\}$ which means we have p distinct choices for each of a, b, hence p^2 total elements in our ring. □

Exercise 9.2.5. *Exhibit all the ideals in the ring $F[x]/(p(x))$, where F is a field and $p(x)$ a polynomial in $F[x]$.*

Factor $p(x)$ into irreducibles $p(x) = q_1(x) \cdots q_k(x)$. Then since the ideals in $F[x]/(p(x))$ are of the form $I/(p(x))$ for any ideal I in $F[x]$ s.t. $(p(x)) \subset I$. Then all ideals are of the form $(\Pi^r q_i(x))/(p(x))$ where $r \leq k$.

Exercise 9.2.9. *Determine the greatest common divisor of* $a(x) = x^5+2x^3+x^2 = x+1$ *and the polynomials* $b(x) = x^5 + x^4 + 2x^3 + 2x^2 + 2x + 1$ *in* $\mathbb{Q}[x]$ *and write it as a linear combination.*

We compute the gcd:

$$\begin{aligned} b(x) &= a(x) + x^4 + x^2 + x, \\ a(x) &= x(x^4 + x^2 + x) + x^3 + x + 1, \\ x^4 + x^2 + x &= x(x^3 + x + 1), \end{aligned} \tag{5}$$

and thus the gcd is $x^3 + x + 1$. So we write:

$$\begin{aligned} x^3 + x + 1 &= a(x) - x(x^4 + x^2 + x) \\ &= a(x) - x(b(x) - a(x)) \\ &= (x + 1)a(x) - xb(x). \end{aligned} \tag{6}$$

and so we've written the gcd as a linear combination of $a(x), b(x)$.

Exercise 9.3.4. *Let* $R = \mathbb{Z} + x\mathbb{Q}[x] \subset \mathbb{Q}[x]$ *be the set of polynomials in* x *with rational coefficients whose constant terms is an integer.*

(a) *Prove that* R *is an integral domain and its units are* ± 1.

Proof. Note that $\mathbb{Q}$ is a field, hence $\mathbb{Q}[x]$ is a PID, and thus an integral domain, and since R is a subset of this integral domain, it too can't possibly have any zero divisors, hence it is also an integral domain. Also since the units in $\mathbb{Q}[x]$ are just the elements of $\mathbb{Q}$, since $\mathbb{Q}$ is a field, we know that the units in R must also be constant terms, and the only integers with inverses are ± 1, hence these are the units in R. $\square$

(b) *Show that the irreducibles in* R *are* $\pm p$ *where* p *is a prime in* $\mathbb{Z}$ *and the polynomials* $f(x)$ *which are irreducible in* $\mathbb{Q}[x]$ *and have constant term* ± 1. *Prove that these irreducibles are prime in* R.

Proof. As noted above, $\mathbb{Q}[x]$ must be a PID, and thus we have that it is also a UFD, and so by Proposition 8.3.12, every irreducible element is also prime. Let $f(x) \in R$ be irreducible. We first consider the case where f is constant. Then f is an integer, and so since we already know the units are ± 1 in R, exactly the primes in $\mathbb{Z}$ are irreducible in this case. Now suppose that $f(x)$ is a nonconstant polynomial, and let the constant term $a_0 \neq \pm 1$. If the constant terms is 0, we can divide by x, which is not a unit, and in the case where $f(x) = \alpha x$, we know $\alpha x = \alpha \frac{1}{2} x$, and so αx is not irreducible. Then clearly we may divide by $|a_0|$, and since all the other coefficients are rationals, we have constructed some $g(x) \neq \pm 1$ s.t. $f(x) = |a_0| g(x)$, i.e. f is the product of two non-units, hence reducible. Thus we must have that $a_0 = \pm 1$ if and only if f is irreducible in this case. $\square$

(c) *Show that* x *cannot be written as the product of irreducibles in* R *(in particular,* x *is not irreducible) and conclude that* R *is not a UFD.*

Proof. Let $f, g, ..., h$ be irreducibles in R. But then we cannot have any non-constant terms, since that would imply a degree ≥ 2 by part (b), so all are constant, which is impossible, so x is not a product of irreducibles. And we proved in part (b) that x is not irreducible, and so R cannot be a UFD since x cannot be written as a product of primes. $\square$

(d) *Show* x *is not a prime and describe* $R/(x)$.

Proof. Suppose x were a prime. Then since R is an integral domain, x would also be irreducible, but it's not, so it can't be. $\square$

$R/(x) = \{ax + b : a \in \mathbb{Q}, b \in \mathbb{Z}\}$. Every non-unit is a zero divisor, since we can multiply by $\frac{1}{b}x$. Hence we are not in an integral domain, but we do have ± 1 units and the ring is still commutative.

Exercise 9.5.5. *Prove that $\sum \phi(d) = n$ where d runs through the divisors of n.*

Proof. Consider $\mathbb{Z}_n$. Let $d|n$, then write $n = dk$, and consider $\langle k \rangle$. This a cyclic subgroup of order d. This subgroup is unique because if it were not, we would have l a generator of another subgroup of order d in $\mathbb{Z}_n$, hence $dk \equiv dl \equiv 0 \mod n$, and since d is the minimal integer such that $dk \equiv 0 \mod n$, we must have that $dk|dl$, but this is also true for l, so $dl|dk$ and so $dk = dl$ and $l = k$, a contradiction. And so the number of elements of order d in R is $\phi(d)$, since $\mathbb{Z}_d$ has exactly that many generators, and we have only one such subgroup. If there were another element of order d not in $\langle k \rangle$, it would form another subgroup which is impossible. Hence since every integer from 1 to n is an element of order d for some $d|n$ we have the desired equality. $\square$