Homework 12

73. We prove that the ideal $I = (2, x)$ within $\mathbb{Z}[x]$ is not principal. We must show there is no $a \in \mathbb{Z}[x]$ such that for all $i \in I$, there is some $r \in \mathbb{Z}[x]$ such that $i = ra$. Suppose it is principal, $I = (a)$.

    Since $2 \in I$, a must be a constant polynomial, otherwise we could never lower its degree to get 2 from multiplying by elements in $\mathbb{Z}[x]$. Then a must be 2, since it is not 1 as I is proper, and it cannot be greater than 2 or we could not generate 2. But then we have no way to generate x, giving a contradiction. Then I cannot be principal.

74. Let $p, r \in \mathbb{N}$ with p prime and $r > 0$. For any a element of $\mathbb{Z}/p^r\mathbb{Z}$ which is relatively prime with p, by reversing the euclidean algorithm, a result commonly referred to as "bezout's identity," as has been verified and discussed in class, there exist integers k and ℓ such that $ka + \ell p = 1$. In other words, there is an integer k such that ka equals 1 mod p. Then a is a unit. Otherwise, if a has a factor of p, we will never get 1 by multiplying it by any other element as 1 has no factor of p. Then the elements of the group of units are precisely those which have no factors of p.

    I was not able to show the cyclicity.

75. Letting $i = \sqrt{-1}$, we first verify that the function $N : \mathbb{Z}[i] \to \mathbb{N}$ is multiplicative: For elements $(a + bi)$ and $(c + di)$, we have

$$\begin{aligned} N((a+bi)(c+di)) &= N((ac-bd)+(ad+bc)i) \\ &= a^2c^2 - 2acbd + b^2d^2 + a^2d^2 + 2adbc + b^2c^2 \\ &= (a^2+b^2)(c^2+d^2) = N(a+bi)N(c+di). \end{aligned}$$

    To find the units, suppose $a, b \in \mathbb{Z}[i]$ with $ab = 1$. Then $N(a)N(b) = N(1) = 1$, and thus we must have $N(a) = N(b) = \pm 1$. Moreover, suppose $N(c) = 1$ for some $c \in \mathbb{Z}[i]$. Then it is clear that c must equal $\pm i$ or ± 1, each of these being units. Then the units of $\mathbb{Z}[i]$ are only those with norm 1.

    Now suppose that $N(\alpha) = p$ for p a prime. Then suppose β, γ exist such that $\beta\gamma = \alpha$. Then $N(\beta)N(\gamma) = N(\alpha) = p$, so that one of $N(\beta)$ and $N(\gamma)$ must be a unit. Thus α is irreducible.

    Finally suppose $N(\alpha) = p^2$ for a prime p such that $p = 3 \mod 4$. Suppose there exist non-units β and γ such that $\beta\gamma = \alpha$. Then we must have $N(\beta) = N(\gamma) = p$. This means that there are integers a and b such that $a^2 + b^2 = p = 3 \mod 4$. Since p is prime, we must have $a, b \neq 0$, otherwise p would be a square. We must also have that one of a and b must be odd and the other even-say a is odd without loss of generality.

    Then $b = 2r$ for an integer r and $a = 2s + 1$. Then we have

$$a^2 + b^2 = 4r^2 + 1 + 4s + 4s^2,$$

    contradicting that $p = 3 \mod 4$, and thus α must be irreducible.

76. We will show $\mathbb{Z}[i]$ is a unique factorization domain by showing it is a euclidean domain, since every euclidean domain is a unique factorization domain.

    Take $a, b \in \mathbb{Z}[i]$. We want to find elements $q, r \in \mathbb{Z}[i]$ such that $a = qb + r$, where either $N(r) < N(b)$ or $r = 0$.

    First note that multiplication by an element of $\mathbb{Z}[i]$ consists of the sum of multiplication by a scalar part and an imaginary part. The product with the imaginary component will be a vector perpendicular to the product with the real component. Then it is clear that multiples of b lie on the square lattice generated by b.

If the point a lies on one of these lattice points, and we can take q to be the gaussian integer which takes b to this point and r to be zero. Otherwise, a lies within on of the lattice boxes. Each point within the lattice can be reached by adding a gaussian integer to a lattice point. We just need to make sure it can be reached by an element of norm less than b. But this is clear, since in the worst case, a lies in the middle of one of these boxes, and the distance from a to any lattice point is still less than the length of b, and otherwise a lies within a ball of radius of less than $\sqrt{2}/2$ times the length of b about some lattice point. Take r to be this difference between a and its closest lattice point to have the desired expression of a.

77. We prove that every prime p which is congruent to 1 modulo 4 is the sum of two squares.

    We have that 4 divides $p-1$ by hypothesis. The group of units of $\mathbb{Z}_p^\times$ is cyclic, and thus there is an element $x \in \mathbb{Z}_p^\times$ such that the powers of x generate the entire group. Since $x^{p-1/2}$ is order 2, it must equal negative one. This is because if $x^2-1=0$, then either $x=-1$ or 1. But it is not 1.

    Then since $p = 1 \mod 4$, the element $x^{p-1/4} = a$ is a square root of -1, and p divides $(a^2+1) = (a+i)(a-i)$. Then p divides one of these terms.

    If $(r+si)p = a+i$, then $rp+spi = a+i$. But this is impossible. Likewise for the other term. Thus p is not prime in $\mathbb{Z}[i]$, and thus is reducible since $\mathbb{Z}[i]$ is a UFD.

78. Let R be a commutative ring and $S \subset R$ a multiplicatively closed subset. We identify the kernel of the map $\iota : R \to R[S^{-1}]$.

    First suppose that $r \in \ker(\iota)$, so that $\iota(r) = 0s/s$ for $s \in S$. Then $rs/s = 0s/s$, and thus $t(rs^2) = 0$ for $t \in S$. Then since R is commutative, $r(ts^2) = 0$, and r is a zero divisor with $q = ts^2 \in S$ such that $rq = 0$.

    Conversely suppose that $r \in R$ such that there exists $s \in S$ with $rs = 0$. Then $rs/s = 0s/s$, since $rs^2 = 0$.

    Then the kernel of ι are those elements $r \in R$ for which there is an element $s \in S$ such that $rs = 0$.

79. Let S be a multiplicatively closed subset of an integral domain R with $0 \notin S$. Note that since $0 \notin S$, the ring $R[S^{-1}]$ is nontrivial. Let P' be an ideal in $R[S^{-1}]$. Then $\iota^{-1}(P') = P$ is an ideal in R, and thus there is some $a \in R$ such that $P = (a)$. Moreover, $P' = (a)[S^{-1}] = \{ra/s : r \in R, s \in S\} = \{a/q \cdot rq/s : r \in R, s \in S\} = (a)$ for any $q \in S$. Then P' is principal.

80. Let $S \subset R$ be a submonoid that does not contain 0. Let P be a maximal element in the set of ideals which do not meet S. Suppose $ab \in P$ but $a, b \notin P$. Then $P + (a)$ and $P + (b)$ must meet S, since they are ideals containing P. Then there exist $r, s \in R$ and $p, q \in P$ such that $p + ra$ and $q + sb$ are in S. But then their product, $pq + qra + psb + rsab$, is both an element of S, since S is closed under multiplication, and an element of P, since P is an ideal. Then this is a contradiction, and either a or b is in P. Then P is prime.

81. Let $p \in \mathbb{Z}$ be a prime number. The canonical map $\varphi : \mathbb{Z} \to \mathbb{Z}_p$ sends every element of $\mathbb{Z} \setminus (p)$ to a unit. Then by the universal property of rings of fractions, there is a map $\psi : \mathbb{Z}_{(p)} \to \mathbb{Z}_p$ such that $\psi \circ \iota = \varphi$.

82. Suppose R is a commutative ring. We will show R is local if and only if for every $r, s \in R$, if $r + s = 1$, then either r or s is a unit.

    First suppose R is local with unique maximal ideal M. Take $r, s \in R$ such that $r + s = 1$, and suppose neither is a unit. Then (r) and (s) are proper ideals and are thus contained in M. But then $r + s = 1 \in M$, and thus $M = R$ giving a contradiction. So one of r and s must be a unit.

    Conversely suppose the latter condition holds. Let A be one maximal ideal and suppose B is another ideal not contained in A. Then $B + A$ contains A and must be equal to R. But then there exist $a \in A$ and $b \in B$ such that $a + b = 1$, thus either a or b is a unit. But A is proper, so b must be a unit and $B = R$. Then the only ideals not contained in A are R, and A is the unique maximal ideal.