Good.

Homework 1 Solutions

January 28, 2019

Also without proof.

Lemma. In the ring $\mathcal{O}$ of integers of a number field, show that if $\alpha \in \mathcal{O}$ has norm equal to a prime of $\mathbb{Z}$, then α is irreducible.

Proof. Let $\mathcal{O}$ be the ring of integers of a number field N and choose $\alpha \in \mathcal{O}$ such that $N(\alpha) = p$ for some prime in $\mathbb{Z}$. Note that I assert without proof that the norm of any unit in $\mathcal{O}$ is an integer. Note also that I assume the norm is multiplicative. We will show that α is irreducible by contradiction. Then assume $\alpha = \beta\gamma$ for β, γ not units and nonzero and note that $p = N(\alpha) = N(\beta\gamma) = N(\beta)N(\gamma)$. Noting that p is irreducible in the integers it follows that one of $N(\beta), N(\gamma)$ is a unit, i.e. ± 1. But this implies that either β or γ is a unit which is a contradiction. □ ✓

This must be Jeremy.

Spelling 1.7. Show that $\mathbb{Z}[i]$ is a principle ideal domain. pal

square too.

Proof. Let I be an ideal of $\mathbb{Z}[i]$ and choose $\alpha \in I$ such that $N(\alpha)$ is minimized. Note that since I is an ideal, $(\alpha) \subseteq I$. We will show that $I \subseteq (\alpha)$. Note that we may create a grid, call it G, that covers $\mathbb{Z}[i]$ by taking the corners of the rhombus formed by $0, \alpha, i\alpha, (1+i)\alpha$ and multiplying by scalars. Then suppose there is a $\beta \in I$ such that $\beta \notin (\alpha)$. Then β is not a grid point in G so we may choose the grid point, γ, such that $N(\gamma - \beta)$ is minimized. Then since β was not a grid point and γ was chosen to minimize the norm of the difference, it follows that $N(\gamma - \beta) <$N(α) and this is a contradiction since we chose α with minimal norm. Therefore, $I = (a)$ and $\mathbb{Z}[i]$ is a PID. □ ✓

1.8. We will use unique factorization in $\mathbb{Z}[i]$ to prove that every prime $p \equiv 1 \pmod 4$ is a sum of two squares.

a. (result) $p \equiv 1 \pmod 4$ implies $n^2 \equiv -1 \pmod p$ from some $n \in \mathbb{Z}$.

b. Prove that p cannot be irreducible in $\mathbb{Z}[i]$.

Proof. Note that since $p | n^2 + 1 = (n+i)(n-i)$ we have that $p | n+i$ or $p | n-i$. But $p \not| n \pm i$ since $p \not| \pm 1$. Therefore, p is not prime in $\mathbb{Z}[i]$ and it follows that p is not irreducible since $\mathbb{Z}[i]$ is a UFD. □ ?! Not enough detail.

HA 1.9. Describe all irreducible elements in $\mathbb{Z}[i]$.

Proof. The irreducible elements of the Gaussian integers are all α such that $N(\alpha) = p$ for prime p and all α such that $N(\alpha) = p^2$ for prime $p \equiv 3 \pmod 4$. □

1.12. Let $\alpha \in \mathbb{Z}[\omega]$. Show that α is a unit iff N$(\alpha) = 1$, and find all units in $\mathbb{Z}[\omega]$.

$\in \mathbb{Z}[i]$

Proof. ($\implies$) Suppose α is a unit. Then for some α', $\alpha\alpha' = 1$. Then $N(\alpha)|1$ and since $N(\alpha) = x^2 + y^2$ for some $x, y \in \mathbb{C}$ we see that $N(\alpha) >= 0$ and so $N(\alpha) = 1$. ($\impliedby$) Suppose $N(\alpha) = 1$. Then $\alpha\overline{\alpha} = 1$ and α is a unit. ✓ □

1.13. Show that $1 - \omega$ is irreducible in $\mathbb{Z}[\omega]$, and that $3 = u(1-\omega)^2$ for some unit u.

↓ use the Lemma. You are reproving it here.

Proof. Suppose for the sake of conradiction that $1-\omega$ is reducible. Then $1-\omega = ab$ for some $a, b \in \mathbb{Z}[\omega]$. It follows that $N(1-\omega) = 3 = N(ab) = N(a)N(b)$ and since 3 is prime in the integers we see that either a or b must be a unit and thus a contradiction, so $1-\omega$ is irreducible in $\mathbb{Z}[\omega]$.

Note that $(1-\omega)^2 = 1 - 2\omega + w^2 = 1 - 2\omega - 1 - \omega = -3\omega$. So let $u = -\overline{\omega}$ and note that $u(1-\omega)^2 = -\overline{\omega}(-3\omega) = 3$ as desired. □

1.15. Here is a proof of Fermat's conjecture for $n = 4$: If $x^4 + y^4 = z^4$ has a solution in positive integers, then so does $x^4 + y^4 = w^2$. Let x, y, w be a solution with smallest possible w. Then x^2, y^2, w is a primitive Pythagorean triple. Assuming (without loss of generality) that x is odd, we can write

$$x^2 = m^2 - n^2,\ y^2 = 2mn,\ w = m^2 + n^2$$

with m and n relatively prime positive integers, not both odd.

(a) Show that

$$x = r^2 - s^2,\ n = 2rs,\ m = r^2 + s^2$$

with r and s relatively prime positive integers, not both odd.

Proof. Note that since $x^2 = m^2 - n^2$, we have $x^2 + n^2 = m^2$ and since $(m, n) = 1$, x is also relatively prime to m,n and we see x, n, m are a pythagorean triple. Thus $x = r^2 - s^2$, $n = 2rs$, $m = r^2 + s^2$ with r and s relatively prime positive integers, not both odd. □

✓

(b) Show that r, s and m are pairwise relatively prime. Using $y^2 = 4rsm$, conclude that r, s and m are all squares, say a^2, b^2 and c^2.

Proof. Suppose m shares a factor with r or s and without loss of generality assume it shares a factor with r. Then some $\alpha | m, r$ so $\alpha\beta = m$ and $\alpha\gamma = r$ for some β, γ. It follows that since $m = r^2 + s^2$, $m - r^2 = s^2 = \alpha\beta - (\alpha\gamma)^2$ and we see that $\alpha | s^2$ so α also divides s and thus a contradiction since $(r, s) = 1$. Then since $y^2 = 4rsm$ and r, s, m are all relatively prime we see that every factor of r, s, m appears an even number of times and r, s and m are all squares, say a^2, b^2 and c^2. ✓ □

$\alpha | m$ $\alpha | r$ then $\alpha | s^2 = r^2 - m$ $\Rightarrow \alpha | s$ $\Rightarrow$ ✗

(c) Show that $a^4 + b^4 = c^2$, and this contradicts the minimality of w. ↓?

Proof. Note that from $m = r^2 + s^2$ we have $a^4 + b^4 = c^2$. But $c/lec^2 = m < m^2 \leq w$ which is a contradiction since w was supposed to be the smallest solution to an equation of the form $a^4 + b^4 = c^2$. □

okay

* 1.16. Show that

$$(1-\omega)(1-\omega^2)\ldots(1-\omega^{p-1}) = p$$

by considering equation (1.2).

cyclotoMic

Proof. Given equation 1.2, note that $t^p - 1 = (t-1)(t-\omega)\ldots(t-\omega^{p-1})$ implies $\frac{t^p-1}{t-1} = (t-\omega)\ldots(t-\omega^{p-1})$ is the cyclotonic polynomial $\Phi_p(t) = 1 + t + \cdots + t^{p-1}$. Therefore, $(t-\omega)\ldots(t-\omega^{p-1})$ evaluated at $t = 1$ is p so $(1-\omega)(1-\omega^2)\ldots(1-\omega^{p-1}) = p$. From the previous problem, $1 - \omega^{k-1} | p$ so $ywp \in P$ and since w is a unit $yp \in P$. But $z \in P$ since $P | (x + y\omega)$ and $(z, yp) = 1$ so there is a linear combination of z and yp equal to 1 and $1 \in P$ which is a contradiction, since P is prime. □

? REMOVE.

Stop HERE! what is the rest for?

Needs work. Since $y\omega(1-\omega^{k-1}) \in P$ so is

$$y\omega(1-\omega^{k-1})\left[(1-\omega)(1-\omega^2)\cdots(1-\omega^{k-2})(1-\omega^{k})\cdots(1-\omega^{p-1})\right]$$

1.19. Dropping the assumption that $\mathbb{Z}[\omega]$ is a UFD but using the fact that *ideals* factor uniquely (up to order) into prime ideals, show that the principle ideal $(w+y\omega)$ has no prime ideal factor in common with any of the other principal ideals on the left side of the equation

$$(x+y)(x+y/w)\dots(x+y\omega^{p-1}) = (z)^p$$

in which all factors are interpreted as principal ideals.

Proof. Suppose P is a prime ideal dividing $(x+y\omega)$ and is also a factor of $(x+y\omega^k)$ for some $k \neq 1$. Then both $(x+y\omega), (x+y\omega^k)$ are contained in P so $x+y\omega, x+y\omega^k \in P$ and $x+y\omega - x - y\omega^k = y\omega(1-\omega^{k-1}) \in P$. ☒

$y\omega p$

Thus, $yp \in P$ since $w \notin P$. But $(yp, z) = 1$ $\Rightarrow 1 = yps + zt$ for $s,t \in \mathbb{Z}$. Since $yp \in P$ and $z \in P$, $1 \in P$. This is a contradiction

YES: ↘

19. Dropping the assumption that $\mathbb{Z}[\omega]$ is a UFD but using the fact that ideals factor uniquely (up to order) into prime ideals, show that the principal ideal $(x+y\omega)$ has no prime ideal factor in common with any of the other principal ideals on the left side of the equation

$$(x+y)(x+y\omega)\cdots(x+y\omega^{p-1}) = (z)^p$$

in which all factors are interpreted as principal ideals.

Proof. Suppose to produce a contradiction that P is a prime ideal and $P \mid (x+y\omega)$ and $P \mid (x+y\omega^k)$ for some $k \neq 1$. Then $(x+y\omega) \subseteq P$ and $(x+y\omega^k) \subseteq P$. Thus, $x+y\omega \in P$ and $x+y\omega^k \in P$, so

$$(x+y\omega) - (x+y\omega^k) = y\omega(1-\omega^{k-1}) \in P.$$

However, because P is an ideal and has the absorption property, by multiplying by the other factors in the equation from exercise 16, we have that

$$y\omega p \in P.$$

Because P is prime, either $yp \in P$ or $\omega \in P$. However, ω is a unit, and as P is prime, it cannot contain any units. Thus, $yp \in P$.

Clearly, equation (1.1) implies that $z^p \in P$, and because P is prime, $z \in P$. However, yp and z are relatively prime, so $1 = ypm + zn \in P$, contradicting the assumption that P is prime. ☐

26. Show that $x + y\omega \equiv u\alpha^p \mod p$ implies

$$x + y\omega \equiv (x+y\omega^{-1})\omega^k \mod p$$

for some $k \in \mathbb{Z}$.

Proof. Note that because $\alpha^p \equiv a \mod p$ for some $a \in \mathbb{Z}$, we have that

$$(x+y\omega) \equiv ua \mod p.$$

Conjugating both sides, we see that

$$\overline{(x+y\omega)} \equiv \overline{ua} \mod p.$$

Because $x, y, a \in \mathbb{Z}$, we have that this is equivalent to

$$x + y\overline{\omega} \equiv \overline{u}a \mod p,$$

Better ~~$x+y\overline{\omega} \equiv \overline{u}a$~~ $\equiv$ You got it!

and as $\overline{\omega} = \omega^{-1}$, we can simply multiply both sides by $u/\overline{u}$ to obtain Yes!

$$\frac{u}{\overline{u}}(x + y\omega^{-1}) \equiv ua \mod p.$$

Good.

Finally, from our first equation,

$$\frac{u}{\overline{u}}(x + y\omega^{-1}) \equiv (x + y\omega) \mod p,$$

□ ✓

29. Let $\omega = e^{2\pi i/23}$. Verify the product

$$(1 + \omega^2 + \omega^4 + \omega^5 + \omega^6 + \omega^{10} + \omega^{11})(1 + \omega + \omega^5 + \omega^6 + \omega^7 + \omega^9 + \omega^{11})$$

is divisible by 2 in $\mathbb{Z}[\omega]$, although neither factor is. It can be shown that 2 is an irreducible element in $\mathbb{Z}[\omega]$; it follows that $\mathbb{Z}[\omega]$ cannot be a UFD.

Proof. Observe that if we expand this out, we obtain the element

$$1 + \omega + \omega^2 + \omega^3 + \omega^4 + 3\omega^5 + 3\omega^6 + 3\omega^7 + \omega^8 + 3\omega^9 + 3\omega^{10} + 7\omega^{11} + \\ + 3\omega^{12} + 3\omega^{13} + \omega^{14} + 3\omega^{15} + 3\omega^{16} + 3\omega^{17} + \omega^{18} + \omega^{19} + \omega^{20} + \omega^{21} + \omega^{22}. \quad (1)$$

However, we have that $1 + \omega + \cdots + \omega^{22} = 0$, so $\omega^{22} = -(1 + \omega + \cdots + \omega^{21})$. Substituting into (1) above, we obtain

$$2\omega^5 + 2\omega^6 + 2\omega^7 + 2\omega^9 + 2\omega^{10} + 6\omega^{11} + 2\omega^{12} + 2\omega^{13} + 2\omega^{15} + 2\omega^{16} + 2\omega^{17},$$

which is clearly divisible by 2. □ ✓

★★★ 30. Show that two ideals in R are isomorphic as R-modules iff they are in the same ideal class.

Ideas Correct. Writing needs improvement.

Proof. First, suppose I_1 and I_2 are two ideals of R, and that they are in the same ideal class. Then $\alpha I_1 = \beta I_2$ for some $\alpha, \beta \in R$. The let $\varphi : I_1 \to I_2$ be defined by

$\alpha, \beta \neq 0$

$$\varphi(x) = \frac{\alpha x}{\beta}.$$

Note that because $\alpha x \in \alpha I_1 = \beta I_2$, it is divisible by β, so this is a well-defined function. Moreover, it is a linear function with an obvious inverse

You need R-module map.

$$\varphi^{-1}(y) = \frac{\beta y}{\alpha},$$

Let $r \in R$, $x \in I_1$, then $\boxed{\varphi(rx) = \frac{\alpha}{\beta} r(x) = r(\frac{\alpha}{\beta}x) = r\varphi(x)}$.

so φ is an R-module isomorphism between I_1 and I_2.

Next, suppose there exists an R-module isomorphism φ between I_1 and I_2. Choose some $\alpha \in I_1$. Then we claim that $\varphi(\alpha)I_1 = \alpha I_2$. Observe that for $a \in I_1$,

HEAVY use of R-module map.

$$\varphi(\alpha)I_1 \ni \varphi(\alpha)a = \varphi(\alpha a) = \alpha\varphi(a) \in \alpha I_2.$$

?

Because φ is a bijection, it has a well-defined inverse, and by symmetry, $\boxed{\text{this property}}$ holds for $b \in I_2$ as well. Thus, I_1 and I_2 are in the same ideal class group. □

??

31. Show that if A is an ideal in R and if αA is principal for some $\alpha \in R$, then A is principal. Conclude that the principal ideals form an ideal class.

For all $a \in I_1$, $\varphi(\alpha)a = \alpha\varphi(a) \in \alpha I_2$. Thus, $\varphi(\alpha)I_1 \subseteq \alpha I_2$.

For $b \in I_2$, $\alpha b = \alpha\varphi(a)$ for some $a \in I_1$ so $\alpha b = \varphi(\alpha)a \Rightarrow \alpha I_2 \subseteq \varphi(\alpha)I_1$ ✓

$\alpha \neq 0.$

Proof. If αA is principal for $\alpha \in R$, then $\alpha A = (\beta)$ for some $\beta \in R$. Note that $\beta \in \alpha A$, so $\beta = \alpha a$ for some $a \in A$. Thus, $a = \frac{\beta}{\alpha}$, and we claim that $A = (a)$.

To show this, we first observe that clearly $(a) \subseteq A$. So, choose $x \in A$. Then $\alpha x \in \alpha A$, so $\alpha x = \beta z$ for some $z \in R$. But then $x = az$ and $x \in (a)$, so $A \subseteq (a)$, and A is principal. ✓

First, note that $(a) \sim (b)$, as $b(a) = (ab) = a(b)$. Moreover, if I is an ideal and $I \sim (a)$ for some principal ideal (a), then by the results of the first part of this problem, I is in fact principal. Thus, the principal ideals form an ideal class. □ ✓ Nice.

32. Show that the ideal classes in R form a group iff for every ideal A there is an ideal B such that AB is principal.

Proof. Suppose the ideal classes in R form a group. Choose an ideal A and let C_1 be its ideal class. Then there exists another class C_2 such that $C_1C_2 = C_0$ (the equation $ax = b$ is always solvable in a group). If $B \in C_2$, then $AB \in C_0$, i.e., AB is principal. ✓

Conversely, suppose that for each ideal A there is an ideal B such that AB is principal. First, note that the set of ideal classes inherits associativity from ideal multiplication in R. Next, we show that C_0 is in fact an identity. If C_0C_1 for some class C_1, choose $A \in C_1$ and $(1) \in C_0$. Then $(1)A = A \in C_1$, so $C_0C_1 = C_1$. Finally, if C_1 is an ideal class and $A \in C_1$, there exists a B such that AB is principal. If C_2 is the ideal class of B, then $C_1C_2 = C_0$, and inverses exist. Thus, the ideal class group is indeed a group. ✓ □

Note: Wikipedia defines $\sim$ on ideals of R that are NON-ZERO.