MATH4302: Solutions to Assignment I

Zichen Yang

February 2, 2021

This is just a sketch of answers. You should be able to figure out the missing details. Also note that there may be typos or errors. Please feel free to contact me by email(zichenyang.math@gmail.com) if you have any questions or difficulties.

Problem 1. Show that a non-zero commutative ring with finitely many elements is a field if and only if it is an integral domain.

Answer. For the non-very-trivial direction, take any non-zero element a, one has to show that a is a unit. By the finiteness, there must be two equal elements in $\{1, a, a^2, a^3, \ldots\}$, say $a^m = a^n$ for $m > n$. Then, $(a^{m-n} - 1)a^n = 0$. Since there is no zero divisor and $a \neq 0$, one has $a^{m-n} = 1$. If $m - n = 1$, then $a = 1$ is invertible. If $m - n > 1$, then a^{m-n-1} is the inverse of a.

Problem 2. Let $n \in \mathbb{Z}$, $n \neq 0$. Describe all the units in the ring $\mathbb{Z}/n\mathbb{Z}$, and show that every non-zero element in $\mathbb{Z}/n\mathbb{Z}$ is either a unit or a zero divisor.

Answer. By Bézout's identity, $\gcd(n, m) = 1$ if and only if there exists $a, b \in \mathbb{Z}$ such that $an + bm = 1$ if and only if there exists $b \in \mathbb{Z}$ such that $bm \equiv 1 \pmod{n}$ if and only if $\overline{m}$ is a unit.

If $\overline{m}$ is not a unit, then there exists $k \in \mathbb{Z}$ such that $k \mid n$ and $k \mid m$. Clearly $d = n/k$ is non-zero in $\mathbb{Z}/n\mathbb{Z}$. But $\overline{m} \cdot \overline{d} = \overline{m} \cdot \overline{n/k} = \overline{m/k} \cdot \overline{n} = 0$. This shows that $\overline{m}$ is a zero divisor.

Problem 3. Show that $\mathbb{Z}[i]$ is a Euclidean domain.

Answer. It is easy to show that $\mathbb{Z}[i]$ is an integral domain since it is a subring of $\mathbb{C}$. A direct calculation shows that $v(ab) = v(a)v(b) \geq \max(v(a), v(b))$ for $a, b \neq 0 \in \mathbb{Z}[i]$. One only has to show that for $a, b \neq 0 \in \mathbb{Z}[i]$, there exist $m, r \in \mathbb{Z}[i]$ such that $a = bm + r$ and $v(r) < v(b)$. If $m \in \mathbb{Z}[i]$, then r is automatically in $\mathbb{Z}[i]$. Thus, it suffices to find $m \in \mathbb{Z}[i]$ such that $v(a/b - m) = |a/b - m| < 1$. This then becomes purely geometric. Drawing the points of $\mathbb{Z}[i]$ on the complex plane $\mathbb{C}$, one can find that the point in $\mathbb{Z}[i]$ that is closest to $a/b \in \mathbb{C}$ has at most a distance $\sqrt{2}/2$ to a/b. This distance is less than 1. Thus, there is always such an $m \in \mathbb{Z}[i]$. Hence, $\mathbb{Z}[i]$ is a Euclidean domain.

Problem 4. Show that $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain.

Answer. Note that $\mathbb{Z}[\sqrt{2}]$ is not a subring of $\mathbb{C}$. So you have to do some calculations to show that it is a domain. A direct calculation shows that $v(ab) = v(a)v(b) \geq \max(v(a), v(b))$ for $a, b \neq 0 \in \mathbb{Z}[\sqrt{2}]$. One only has to show that for $a, b \neq 0 \in \mathbb{Z}[\sqrt{2}]$, there exist $m, r \in \mathbb{Z}[\sqrt{2}]$ such that $a = bm + r$ and $v(r) < v(b)$. If $m \in \mathbb{Z}[\sqrt{2}]$, then r is automatically in $\mathbb{Z}[\sqrt{2}]$. Thus, it suffices to find $m \in \mathbb{Z}[\sqrt{2}]$ such that $v(a/b - m) < 1$. It can be done as following. Suppose that $a/b = x + iy$, where we only have $x, y \in \mathbb{Q}$.

Then, a simple idea is to take integers $x', y' \in \mathbb{Z}$ such that $|x' - x|, |y' - y| \leq 1/2$. Then, we claim that m can be $x' + y'i$. Indeed,

$$v(a/b - m) = \big||x' - x|^2 - 2|y' - y|^2\big| \leq \frac{3}{4} < 1.$$

Hence, $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain.

Problem 5. For a commutative ring R, denote by $R^\times$ the group of all units in R. Show that the group $(\mathbb{Z}/7\mathbb{Z})^\times$ is cyclic and find one of its generators.

Answer. By direct calculations, it is clearly cyclic. The generator may be $\overline{3}$ or $\overline{5}$.

Problem 6. Describe all the irreducible elements in $\mathbb{Z}[i]$. Classify all prime ideals and all maximal ideals of $\mathbb{Z}[i]$.

Answer. Note that the zero ideal is a special case. It is a prime ideal but not a maximal ideal in $\mathbb{Z}[i]$. Then, we only deal with non-zero ones.

Define $N\colon \mathbb{Z}[i] \to \mathbb{Z}$ the norm map $N(a + bi) = a^2 + b^2$. It is a simple exercise to show that $N(a + bi) = 1$ if and only if $a + bi$ is a unit. We already know that $\mathbb{Z}[i]$ is a PID. So, prime elements are equivalent to irreducible elements. Moreover, in the video lectures, the prime ideals are generated by prime elements. So, it suffices to classify all prime elements. We show that a prime element differs one of the following three types by a unit.

1. $1 + i$;
2. $a + bi$, if $a^2 + b^2 = p$ where p is a prime number and $p \equiv 1 \pmod 4$ (i.e. the remainder of p divided by 4 is 1);
3. p, if p is a prime number and $p \equiv 3 \pmod 4$.

First, we prove that they are indeed prime elements. If $p \equiv 1 \pmod 4$ and $a^2+b^2 = (a+bi)(a-bi) = p$, one has $N(a+ib) = p$. Suppose that $a+bi$ is not a prime element, which has a factoriazation $a + bi = \alpha\beta$. Then $N(\alpha)N(\beta) = p$ implies that either α or β is a unit. Thus, $a + bi$ is a prime element. Since $2 = (1 + i)(1 - i)$, using the same argument, one can show that $1 + i$ are is a prime element. If $p \equiv 3 \pmod 4$, one may suppose that $p = \alpha\beta$ where α, β are non-units in $\mathbb{Z}[i]$. Using the same argument, one has $N(\alpha) = p$. Writing $\alpha = x + yi$. Then, one has $p = N(\alpha) = x^2 + y^2$. But, this is impossible. Indeed, one sees that if x is an integer, then $x^2 \equiv 0, 1 \pmod 4$, where the remainder is 0 if x is an even number, and is 1 if x is an odd number. Thus, one sees that $p = x^2 + y^2 \not\equiv 3 \pmod 4$.

Conversely, if given a prime element $\pi \in \mathbb{Z}[i]$, one has to show that $\pi = a + bi$ is one of the three types times a unit. Suppose that one has the factorization $\pi\overline{\pi} = N(\pi) = p_1 \cdots p_r$ where p_i are prime numbers. Then, WLOG, π divides $p = p_1$ since π is a prime element. Then, $N(\pi)|N(p) = p^2$. Hence, $N(\pi) = p$ or p^2. In the former case, $a^2 + b^2 = p$ gives the first or the second type. In the latter case, $N(p/\pi) = N(p)/N(\pi) = 1$ which implies $\pi = pu$ for some unit $u \in \mathbb{Z}[i]$. Then, we claim that p must be the third type. Otherwise if $p \equiv 1 \pmod 4$ or $p = 2$, $p = \pi u^{-1}$ is a prime element. To raise a contradiction that p is not a prime element, it suffices to show that $p = x^2 + y^2 = (x + yi)(x - yi)$ where x, y are integers, if $p \equiv 1 \pmod 4$. This is indeed a famous theorem by Fermat.

Remark. To prove Fermat's theorem, one can first prove Wilson's theorem: $(p - 1)! \equiv -1 \pmod p$, if p is a prime number. Indeed, one knows that $\mathbb{Z}/p\mathbb{Z}$ is a field. Thus, all non-zero elements form a group. Consider the product of these non-zero

elements $1 \cdot 2 \cdot \cdots \cdot (p-2) \cdot (p-1)$, each element can be paired with its inverse in the product, except 1 and $p-1$, because they are their own inverses. Hence, $(p-1)! = 1 \cdot 2 \cdot \cdots \cdot (p-2) \cdot (p-1) \equiv -1 \pmod{p}$. With Wilson's theorem, one can show that $x^2 + 1 \equiv 0 \pmod{p}$ or equivalently $x^2 \equiv -1 \pmod{p}$ has an integer solution if $p \equiv 1 \pmod{4}$. Indeed, if $p \equiv 1 \pmod{4}$, write $p = 1 + 4n$ for some $n \in \mathbb{Z}$. Then by Wilson's theorem, $-1 \equiv (p-1)! = (1 \cdot 2 \cdot \cdots \cdot 2n)((2n+1) \cdot (2n+2) \cdot \cdots \cdot 4n) \equiv (1 \cdot 2 \cdot \cdots \cdot 2n)((-2n) \cdot (-(2n-1)) \cdot \cdots \cdot (-1)) \equiv (-1)^{2n}(2n!)^2 \equiv (2n!)^2 \pmod{p}$. So, $(2n!)$ is the solution to the equation $-1 \equiv x^2 \pmod{p}$. Thus, there exists $x \in \mathbb{Z}$ such that $x^2 + 1 = (x+i)(x-i)$ is divisible by p. But, $x - i$ and $x + i$ are not divisible by p. Thus p is not a prime element in $\mathbb{Z}[i]$. Then, one may suppose that $p = \alpha\beta$ where α, β are non-units. Finally, using the same argument above, one has $N(\alpha) = p$. Writing $\alpha = x + yi$, one has the desired result $x^2 + y^2 = p$.

Problem 7. Describe all the irreducible elements in $\mathbb{R}[x]$; Classify all prime ideals and all maximal ideals of $\mathbb{R}[x]$.

Answer. For a polynomial in $\mathbb{R}[x]$, consider it as a polynomial in $\mathbb{C}[x]$, it can also factor into linear polynomials. Notice that if it has a root in $\tau \in \mathbb{C} - \mathbb{R}$, it must have a conjugate root $\overline{\tau}$. Multiplying the conjagate pair gives you a quadratic polynomial in $\mathbb{R}[x]$. Thus, the set of irreducible elements in $\mathbb{R}[x]$ consists of all linear polynomial and all quadratic polynomial without real roots. Since $\mathbb{R}[x]$ is a PID, except the zero ideal, the set of prime ideals is exactly the set of maximal ideals.

Problem 8. Suppose that R is a PID but is not a field. Show that $R[x]$ is not a PID.

Answer. Since R is not a field, one may take a non-zero non-unit $a \in R$. Then, one claims that the ideal generated by a and x is not principal. The general element in this ideal is of the form $af(x) + xg(x)$ such that $f, g \in R[x]$. Thus, it can not generate $1 \in R$ since a is a non-unit. Hence, it can not be $R[x]$.

Now, suppose that it is principal, say, generated by $h(x)$. Then, $x = h(x)j(x)$ for some $j(x)$. By counting the degree, $h(x)$ can either be bx such that b is a unit, or a unit c. However, in the former case a is not in the ideal generated by $h(x)$ while in the latter case, the ideal is $R[x]$.

Remark. The above is my solution. There is another much better solution from a previous student. Suppose the contrary. Then, the ideal (x) is obviously seen to be a prime ideal, thus a maximal ideal. Then, the quotient $R[x]/(x) \simeq R$ is a field. Contradition!

Problem 9. Describe all ideals, prime ideals, and maximal ideals of the ring $\mathbb{Z}/n\mathbb{Z}$ for any integer $n \geq 2$.

Answer. Let R be a ring and I be an ideal of R. Let $\pi \colon R \to R/I$ be the homomorphism which maps r to $r + I$. Given an ideal J of R containing I, show that the image $\pi(J)$ is an ideal of R/I. Conversely, given an ideal $\bar{J}$ of R/I, show that the preimage $\pi^{-1}(\bar{J})$ is an ideal of R containing I. Then, this gives a one-to-one correspondence between ideals of R containing I and ideals of R/I. Moreover, prime ideals and maximal ideals are correspondent to prime ideals and maximal ideals. For a proof, see the webpage.

https://math.stackexchange.com/questions/69578

This question is a special case $R = \mathbb{Z}$ and $I = n\mathbb{Z}$. The ideals are generated by a single element $\overline{m}$ such that $m \mid n$. The prime ideals and maximal ideals are generated by $\overline{p}$ where p is a prime factor of n.

Problem 10. Compute a greatest common divisor in $\mathbb{Z}[i]$ of $14 + 2i$ and $21 + 26i$.

Answer. Computing the norms of these two elements, $N(14 + 2i) = 200 = 2^3 5^2$ and $N(21 + 26i) = 1117$ is a prime number. Since $1117 \equiv 1 \pmod 4$, $21 + 26i$ is a prime element. Thus, the greatest common divisor of them could be $21 + 26i$ or 1. Clearly, $14+2i$ is not divisible by $21+26i$ by looking at the norms. Thus, a choice of a greatest common divisor may be $\pm 1, \pm i$.