(*October 17, 2023*)

Discussion 02

Paul Garrett garrett@umn.edu https://www-users.cse.umn.edu/~garrett/

[02.1] Find all the idempotent elements in $\mathbb{Z}[i]/\langle 13\rangle$.

Implicit in the question is that the method should scale well, so "brute force" is an unhelpful response. To begin with, there are 169 elements in that quotient ring...

Discussion: To get oriented, we *might* first want to see whether the rational prime 13 is still prime/irreducible in $\mathbb{Z}[i]$. One approach to this is to use an isomorphism theorem:

$$\mathbb{Z}[i]/\langle 13\rangle \;\approx\; \mathbb{Z}[x]/\langle x^2+1, 13\rangle \;\approx\; (\mathbb{Z}/13)[x]/\langle x^2+1\rangle$$

We might remember (from a forward reference?) that, since finite subgroups of multiplicative groups of fields are cyclic, there is $\sqrt{-1}$ in a finite field with q elements if and only if $q = 1 \bmod 4$. Since 13 is prime, $\mathbb{Z}/13$ is a field. Since $13 = 1 \bmod 4$, there is a $\sqrt{-1}$ in $\mathbb{Z}/13$, so x^2+1 factors, even though this line of thought does not immediately tell what $\pm\sqrt{-1}$ is in $\mathbb{Z}/13$. Further, even without knowing what $\sqrt{-1} \in \mathbb{Z}/13$ is, we can check that the two linear factors $x \pm \sqrt{-1}$ are relatively prime in $\mathbb{Z}/13[x]$, via the Euclidean algorithm there:

$$(x-\sqrt{-1}) - 1\cdot(x+\sqrt{-1}) \;=\; -2\cdot\sqrt{-1}$$

Since neither $\sqrt{-1}$ nor 2 are divisible by (the prime) 13, $-2\cdot\sqrt{-1}$ is a unit in the field $\mathbb{Z}/13$, so $x \pm \sqrt{-1}$ are coprime, in case we were worried.

Thus, by Sun-Ze's theorem,

$$(\mathbb{Z}/13)[x]/\langle x^2+1\rangle \;\approx\; (\mathbb{Z}/13)[x]/\langle x-\sqrt{-1}\rangle \oplus (\mathbb{Z}/13)[x]/\langle x+\sqrt{-1}\rangle$$

In particular, this quotient is not a domain, so 13 is not prime/irreducible in $\mathbb{Z}[x]$.

This is good to know. However, that previous discussion does not seem to give an *optimal* approach to finding idempotents in that quotient. Of course, we might only find that out after trying more than one approach, which entails some inefficiencies *anyway*. After some experimentation, perhaps the following is the optimal approach, in the sense of scaling well.

If we remember the Fermat theorem on primes which are sums of two squares, then since $13 = 1 \bmod 4$ we know that $13 = a^2 + b^2$ for some integers a, b. To find them, we have a quite small search space (in comparison to looking for $\sqrt{-1} \bmod 13$ naively), namely, on the order of $\sqrt{13}$ things to try. We find $13 = 3^2 + 2^2 = (3+2i)(3-2i)$. Both to check that $3 \pm 2i$ are coprime, and to get the coefficients for the extended Euclidean algorithm/Sun-Ze: in the forward direction, the Euclidean algorithm is

$$\begin{array}{rcl} (3+2i) - i\cdot(3-2i) & = & 1-i \\ (3-2i) - 2\cdot(1-i) & = & 1 \end{array}$$

verifying that the $3 \pm 2i$ are relatively prime. Going back,

$$1 \;=\; (3-2i) - 2\cdot(1-i) \;=\; (3-2i) - 2\cdot[(3+2i) - i\cdot(3-2i)] \;=\; (-2)\cdot(3+2i) + (1+2i)\cdot(3-2i)$$

Recall that the formula for x such that $x = a \bmod m$ and $x = b \bmod n$, with $\gcd(m,n) = 1$ and $rm+sn = 1$, is $x = brm + asn \bmod mn$. The two non-trivial idempotents (that is, other than $0, 1$) will be $x = 0 \bmod 3+2i$ and $x = 1 \bmod 3-2i$, and $x = 1 \bmod 3+2i$ and $x = 0 \bmod 3-2i$. Plugging in, the two non-trivial idempotents are

$$\begin{cases} x &= 1\cdot(-2)\cdot(3+2i) + 0\cdot(1+2i)\cdot(3-2i) &= -6-4i \\ x &= 0\cdot(-2)\cdot(3+2i) + 1\cdot(1+2i)\cdot(3-2i) &= 7+4i \end{cases}$$

Of course, $-6 = 7 \bmod 13$, etc. ///

[02.2] Find all the nilpotent elements in $\mathbb{Z}[i]/\langle 2\rangle$.

Discussion: At the beginning, there are two slightly different approaches. One is to accidentally observe that $2 = (1+i)\cdot(1-i)$, so 2 is *not* a prime in $\mathbb{Z}[i]$. Indeed, $1+i = i\cdot(1-i)$, so $1 \pm i$ are *associates*, in the sense that they are irreducibles/primes just differing by a (multiplicative) unit.

Abstracting a bit, for a commutative ring R (with 1), maybe a UFD to make things very simple, R/p^2 (with p a prime) has easily described idempotents. Namely, exactly things in $R \cdot p$. To prove this: if $r \in R$ is *not* divisible by p, then no power r^n will be so, much less divisible by p^2. On the other hand, if $p|r$, then $r^2 = 0 \bmod p^2$. ///

[02.3] *(Lagrange interpolation)* Let $\alpha_1, \ldots, \alpha_n$ be *distinct* elements in a field k, and let $\beta_1, \ldots, \beta_n$ be any elements of k. Prove that there is a unique polynomial $P(x)$ of degree $< n$ in $k[x]$ such that, for all indices i,

$$P(\alpha_i) \;=\; \beta_i$$

Indeed, letting

$$Q(x) \;=\; \prod_{i=1}^{n} (x - \alpha_i)$$

show that

$$P(x) \;=\; \sum_{i=1}^{n} \frac{Q(x)}{(x-\alpha_i)\cdot Q'(\alpha_i)} \cdot \beta_i$$

Discussion: Since the α_i are distinct,

$$Q'(\alpha_i) = \prod_{j\neq i} (\alpha_i - \alpha_j) \neq 0$$

(One could say more about purely algebraic notions of derivative, but maybe not just now.) Evaluating $P(x)$ at $x \to \alpha_i$,

$$\frac{Q(x)}{(x-\alpha_j)} \;\text{ evaluated at } x \to \alpha_i \;= \begin{cases} 1 & (\text{for } j = i) \\ 0 & (\text{for } j = i) \end{cases}$$

Thus, all terms but the i^{th} vanish in the sum, and the i^{th} one, by design, gives β_i. For uniqueness, suppose $R(x)$ were another polynomial of degree $< n$ taking the same values at n distinct points α_i as does $Q(x)$. Then $Q - R$ is of degree $< n$ and vanishes at n points. A non-zero degree ℓ polynomial has at most ℓ zeros, so it must be that $Q - R$ is the 0 polynomial. ///

[02.4] *(Simple case of partial fractions)* Let $\alpha_1, \ldots, \alpha_n$ be *distinct* elements in a field k. Let $R(x)$ be any polynomial in $k[x]$ of degree $< n$. Show that there exist unique constants $c_i \in k$ such that in the field of rational functions $k(x)$

$$\frac{R(x)}{(x-\alpha_1)\ldots(x-\alpha_n)} = \frac{c_1}{x-\alpha_1} + \ldots + \frac{c_n}{x-\alpha_n}$$

In particular, let

$$Q(x) = \prod_{i=1}^{n} (x - \alpha_i)$$

and show that

$$c_i = \frac{R(\alpha_i)}{Q'(\alpha_i)}$$

Discussion: We might emphasize that the field of rational functions $k(x)$ is most precisely the *field of fractions* of the polynomial ring $k[x]$. Thus, in particular, equality $r/s = r'/s'$ is exactly equivalent to the equality $rs' = r's$ (as in elementary school). Thus, to test whether or not the indicated expression performs as claimed, we test whether or not

$$R(x) = \sum_i \left(\frac{R(\alpha_i)}{Q'(\alpha_i)} \cdot \frac{Q(x)}{x - \alpha_i} \right)$$

One might notice that this is the previous problem, in case $\beta_i = R(\alpha_i)$, so its correctness is just a special case of that, as is the uniqueness (since $\deg R < n$). ///

[02.5] Show that the ideal I generated in $\mathbb{Z}[x]$ by $x^2 + 1$ and 5 is *not* maximal.

Discussion: We will show that the quotient is not a field, which implies (by the standard result proven above) that the ideal is not maximal (proper).

First, recall that the quotient of a ring R by an ideal $I = Rx + Ry$ generated by two elements can be expressed as a two-step quotient, namely

$$(R/\langle x\rangle)/\langle \bar{y}\rangle \;\approx\; R/(Rx + Ry)$$

where the $\langle \bar{y}\rangle$ is the principal ideal generated by the *image* $\bar{y}$ of y in the quotient $R/\langle x\rangle$. The principal ideal generated by y in the quotient $R/\langle x\rangle$ is the set of cosets

$$\langle \bar{y}\rangle \;=\; \{(r + Rx) \cdot (y + Rx) : r \in R\} \;=\; \{ry + Rx : r \in R\}$$

noting that the multiplication of cosets in the quotient ring is *not* just the element-wise multiplication of the cosets. With this explication, the natural map is

$$r + \langle x\rangle \;=\; r + \langle x\rangle \;\longrightarrow\; r + \langle x\rangle + \langle y\rangle' \;=\; r + (Rx + Rx)$$

which is visibly the same as taking the quotient in a single step.

Thus, first

$$\mathbb{Z}[x]/\langle 5\rangle \;\approx\; (\mathbb{Z}/5)[x]$$

by the map which reduces the coefficients of a polynomial modulo 5. In $(\mathbb{Z}/5)[x]$, the polynomial $x^2 + 1$ *does* factor, as

$$x^2 + 1 \;=\; (x - 2)(x + 2)$$

(where these 2s are in $\mathbb{Z}/5$, not in $\mathbb{Z}$). Thus, the quotient $(\mathbb{Z}/5)[x]/\langle x^2 + 1\rangle$ has proper zero divisors $\bar{x} - 2$ and $\bar{x} + 2$, where $\bar{x}$ is the image of x in the quotient. Thus, it's not even an integral domain, much less a field. ///

[02.6] Show that the ideal I generated in $\mathbb{Z}[x]$ by $x^2 + x + 1$ and 7 is *not* maximal.

Discussion: As in the previous example, compute the quotient in two steps. First,

$$\mathbb{Z}[x]/\langle 7\rangle \;\approx\; (\mathbb{Z}/7)[x]$$

by the map which reduces the coefficients of a polynomial modulo 7. In $(\mathbb{Z}/7)[x]$, the polynomial $x^2 + x + 1$ *does* factor, as

$$x^2 + x + 1 \;=\; (x - 2)(x - 4)$$

(where 2 and 4 are in $\mathbb{Z}/7$). Thus, the quotient $(\mathbb{Z}/7)[x]/\langle x^2 + x + 1\rangle$ has proper zero divisors $\bar{x} - 2$ and $\bar{x} - 4$, where $\bar{x}$ is the image of x in the quotient. Thus, it's not even an integral domain, so certainly not a field.

[02.7] Let k be a field. Given $P \in k[x]$ of degree n, show that there is a k-linear map $T : k^n \to k^n$ such that $P(T) = 0$.

Discussion: There is no need to explicitly mention k^n, since any n-dimensional k-vectorspace has many isomorphisms to k^n, by any choices of basis. In particular, it is somewhat advantagous to delay choice-of-basis.

By the way, since k is not assumed to be algebraically closed, there are obstacles to just letting T by scalar multiplication by λ, where λ is a root of $P(x) = 0$.

Let $V = k[x]/\langle P\rangle$. Since P has degree n, there *is* a basis $1, x, x^2, \ldots, x^{n-1}$ for that vectorspace quotient, so V is indeed n-dimensional. Let $T : V \to V$ be multiplication by x (on the quotient). The property $P(T) = 0$ is easy: for any $v \in k[x]$, representing an element in the quotient,

$$P(T)(v) \;=\; P(x) \cdot v + \langle P(x)\rangle \;\in\; \langle P(x)\rangle \;=\; 0$$

noting that the "vector" v itself is in a quotient of $k[x]$. ///

[02.8] Determine all two-sided ideals in the ring of n-by-n matrices with entries in a field k.

Discussion: Let R be that ring of n-by-n matrices, and I a non-zero ideal. We will show that $I = R$. Let $m \neq 0$ be an element of I.

Since m is not the 0 matrix, it has some non-zero entry m_{ij}, at the ij^{th} place. Left and right multiply by appropriate permutation matrices to move that non-zero entry to the $1,1$ position (for example). Left multiply by a scalar matrix to make the $1,1$ entry simply be 1, for simplicity.

Then right-and-left multiply by suitable upper/lower triangular matrices to make all the other entries in the top row and left-most column 0 (apart from the $1,1$ entry).

The ring R has an obvious subring

$$S \;=\; \begin{pmatrix} 1 & 0 \\ 0 & * \end{pmatrix}$$

with the $*$ being $(n-1)$-by-$(n-1)$. Thus, we can do induction on n. That is, I contains either

$$\begin{pmatrix} 1 & 0 \\ 0 & 0_{n-1} \end{pmatrix} \qquad \text{or} \qquad \begin{pmatrix} 1 & 0 \\ 0 & 1_{n-1} \end{pmatrix}$$

In the latter case, we have $1_n \in I$, so $I = R$, and we're done. In the former, we can add copies of $\begin{pmatrix} 1 & 0 \\ 0 & 0_{n-1} \end{pmatrix}$ left-and-right multiplied by permutation matrices, moving the 1 to all other diagonal positions, to give

$$\begin{pmatrix} 1 & 0 \\ 0 & 0_{n-1} \end{pmatrix} + \begin{pmatrix} 0 & 0 & \ldots \\ 0 & 1 & \ldots \\ 0 & 0 & 0_{n-2} \end{pmatrix} + \ldots \;=\; 1_n$$

Thus, again, $1_n \in I$, so $I = R$. ///

[02.9] Let $V_1 \subset \ldots \subset V_{n-1} \subset V$ and $W_1 \subset \ldots \subset W_{n-1} \subset V$ be two maximal flags in an n-dimensional vector space V over a field k. Show that there is a k-linear map $T : V \to V$ such that $TV_i = W_i$.

[... iou ...] :)
