Math 4520

Fields

Book 1

A <u>field</u> is a number system with $+, -, \times, \div, 0, 1$ in which we can divide by every nonzero element.

$\mathbb{R} = \{\text{real numbers}\}$ is a field

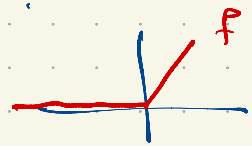
$\mathbb{C} = \{\text{complex numbers}\}$ .. .. $\qquad \mathbb{C} = \{a+bi : a,b \in \mathbb{R}\}, \quad i = \sqrt{-1}$

$\mathbb{Q} = \{\text{rational numbers}\}$ .... $\qquad \mathbb{Q} = \{\frac{a}{b} : a,b \in \mathbb{Z},\ b \neq 0\}$

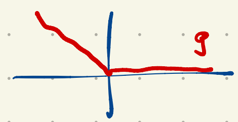
$\mathbb{Z} = \{\text{integers}\} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$ is not a field. $\mathbb{Z}$ is a commutative ring with 1 (having no zero divisors)

Other examples of fields?

$$f(x) = \begin{cases} x, & \text{if } x \geq 0 \\ 0, & \text{if } x < 0 \end{cases}$$



$$g(x) = \begin{cases} 0, & \text{if } x \geq 0 \\ -x, & \text{if } x < 0 \end{cases}$$



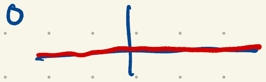
$f(x) + g(x) = |x|$

$f(x) - g(x) = x$

$f(x)g(x) = \underline{0}$

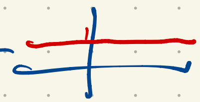
$\cancel{\frac{f(x)}{g(x)}}$

$f \neq 0$



$f(x)$ and $g(x)$ are nonzero functions whose product is 0 (these are called <u>zero divisors</u> in ring theory).

The continuous functions $\mathbb{R} \to \mathbb{R}$ form a commutative ring with identity



but not a field.

$\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$ is a field of <u>order</u> 5.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$3 + 4 = 2$

$3 - 4 = 4$

$3 \times 4 = 2$

$\frac{3}{4} = 2$

$\mathbb{R}, \mathbb{C}, \mathbb{Q}$ are infinite fields; $\mathbb{F}_5$ is a finite field.

In $\mathbb{Z}$, $8 \equiv 3 \bmod 5$. (8 is congruent to 3 mod 5)

In $\mathbb{F}_5$, $8 = 3$.

$$\frac{3}{4} = 2 \iff 3 = 2 \times 4$$

$2 \times 4 = 8 = 3$

Fields

Let F be a set containing distinct elements called 0 and 1 (thus $0 \neq 1$). Suppose addition, subtraction, multiplication and division are defined for all elements of F (except division by 0 is not defined).
Thus $a+b,\ a-b,\ ab,\ \frac{a}{d} \in F$ whenever $a, b, d \in F$ and $d \neq 0$.
Define $-a = 0 - a$.

If the following properties are satisfied by *all* elements $a, b, c, d \in F$ with $d \neq 0$, then F is a field.

$$a + b = b + a \qquad a + (b + c) = (a + b) + c \qquad ab = ba$$

$$a + 0 = a \qquad a(bc) = (ab)c \qquad 1a = a$$

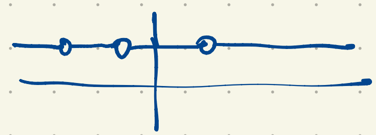
$$a + (-a) = 0 \qquad a(b + c) = ab + ac \qquad \frac{a}{d}d = a$$

$$a + (-b) = a - b$$

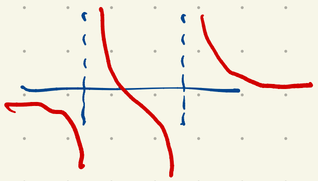
The ring of polynomials in x with real coefficients is $\mathbb{R}[x]$ is a commutative ring with identity having no zero divisors (if $f(x), g(x)$ are nonzero polynomials then $f(x)g(x)$ is a nonzero polynomial)

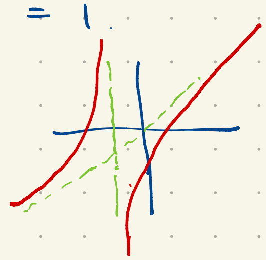
$1 f(x) = f(x)$

$\mathbb{R}(x) = \{$ rational functions in x with real coefficients $\}$, a field.



$$\frac{2x+1}{3x^2-7} \cdot \frac{3x^2-7}{2x+1} = 1$$





$$\mathbb{R}(x) = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in \mathbb{R}[x], \ g(x) \neq 0 \right\}.$$

$$x \cdot \frac{1}{x} = 1$$

$$\mathbb{Q} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, \ b \neq 0 \right\}.$$

$\mathbb{Q}[\sqrt{2}] = \{ a + b\sqrt{2} : a, b \in \mathbb{Q} \}$ is a field.

$$\left.\begin{array}{l} \alpha = 3 + 7\sqrt{2} \\ \beta = 5 - \sqrt{2} \end{array}\right\} \in \mathbb{Q}[\sqrt{2}]$$

$$\alpha + \beta = (3+7\sqrt{2}) + (5 - \sqrt{2}) = 8 + 6\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

$$\alpha - \beta = (3+7\sqrt{2}) - (5-\sqrt{2}) = -2 + 8\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

$$\alpha\beta = (3+7\sqrt{2})(5-\sqrt{2}) = 15 - 3\sqrt{2} + 35\sqrt{2} - 14 = 1 + 32\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

$$\frac{\alpha}{\beta} = \frac{3+7\sqrt{2}}{5-\sqrt{2}} \cdot \frac{5+\sqrt{2}}{5+\sqrt{2}} = \frac{15+3\sqrt{2}+35\sqrt{2}+14}{25-2} = \frac{29+38\sqrt{2}}{23} = \frac{29}{23} + \frac{38}{23}\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

$\mathbb{Q}[i] = \{ a + bi : a, b \in \mathbb{Q} \}$, $i = \sqrt{-1}$. This is a field.

$$\alpha = 1 + \tfrac{1}{3}i, \quad \beta = \tfrac{3}{2} - i \implies$$

$$\alpha + \beta = \tfrac{5}{2} - \tfrac{2}{3}i$$

$$\alpha - \beta = -\tfrac{1}{2} + \tfrac{4}{3}i$$

$$\alpha\beta = \tfrac{3}{2} - i + \tfrac{1}{2}i + \tfrac{1}{3} = \tfrac{11}{6} - \tfrac{1}{2}i \in \mathbb{Q}[i]$$

$$\frac{\alpha}{\beta} = \frac{1+\frac{1}{3}i}{\frac{3}{2}-i} \cdot \frac{6}{6} = \frac{6+2i}{9-6i} \cdot \frac{9+6i}{9+6i} = \frac{54+36i+18i-12}{81+36}$$

$$= \frac{42+54i}{117} = \frac{14}{39} + \frac{18}{39}i \in \mathbb{Q}[i].$$

Example $R = \{ \text{real } 2\times 2 \text{ matrices} \} = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in \mathbb{R} \right\}$. noncommutative ring with identity $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ having zero divisors

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \qquad \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

The subset $F = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} : a,b \in \mathbb{R} \right\} \subset R$ is a subring which is actually a field

$$\det \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = a^2 + b^2 \neq 0 \quad \text{whenever } \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix}^{-1} = \frac{1}{a^2+b^2} \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \quad \ldots\ldots \quad \ldots\ldots$$

$F = \{ aI + bJ : a,b \in \mathbb{R} \}$, $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $J = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ basis for F.

$$J^2 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = -I$$

$$a \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + b \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

$$(aI + bJ)(cI + dJ) = acI + adJ + bcJ + bdJ^2 = (ac - bd)I + (ad+bc)J \in F$$

$$(cI + dJ)(aI + bJ) = (ca - db)I + (cb + da)J$$

All field axioms hold in F, so F is a field.

Rename element $aI + bJ \in F$ $\left(= \begin{bmatrix} a & b \\ -b & a \end{bmatrix},\ a,b \in \mathbb{R} \right)$ as $a \cdot 1 + bi = a + bi \in \mathbb{C}$

In $\mathbb{C}$: $(a+bi)(c+di) = ac + adi + bci - bd = (ac-bd) + (ad+bc)i$

Our example F is essentially the same as $\mathbb{C}$. More precisely, they are isomorphic: we have a bijection $f : \mathbb{C} \to F$, $f(a+bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ for all $a,b \in \mathbb{R}$ such that

$$f(zw) = f(z)f(w), \quad f(z+w) = f(z) + f(w) \quad \text{for all } z,w \in \mathbb{C}.$$

$\mathbb{Q}[i]$ is isomorphic to the ring $E = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} : a, b, c, d \in \mathbb{Q} \right\}$

$$f : \mathbb{Q}[i] \longrightarrow E, \qquad f(a+bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

$\alpha = 1 + \frac{1}{3} i$ $\quad \{1, i\}$ basis for $\mathbb{Q}[i]$ over $\mathbb{Q}$

$\beta = \frac{3}{2} - i$

$$f(\beta) = \begin{bmatrix} 3/2 & -1 \\ 1 & 3/2 \end{bmatrix}$$

$$f(\beta)^{-1} = \begin{bmatrix} 3/2 & -1 \\ 1 & 3/2 \end{bmatrix}^{-1} = \frac{1}{\frac{9}{4}+1} \begin{bmatrix} 3/2 & 1 \\ -1 & 3/2 \end{bmatrix} = \frac{4}{13} \begin{bmatrix} 3/2 & 1 \\ -1 & 3/2 \end{bmatrix}$$

$$f\left(\frac{\alpha}{\beta}\right) = f(\alpha) f(\beta^{-1}) = \frac{4}{13} \begin{bmatrix} 1 & 1/3 \\ -1/3 & 1 \end{bmatrix} \begin{bmatrix} 3/2 & 1 \\ -1 & 3/2 \end{bmatrix} = \frac{4}{13} \begin{bmatrix} 7/6 & 3/2 \\ -3/2 & 7/6 \end{bmatrix} = \frac{4}{13} \cdot \frac{1}{6} \begin{bmatrix} 7 & 9 \\ -9 & 7 \end{bmatrix} = \frac{2}{39} \begin{bmatrix} 7 & 9 \\ -9 & 7 \end{bmatrix} = \frac{1}{39} \begin{bmatrix} 14 & 18 \\ -18 & 14 \end{bmatrix}$$

$$\frac{3}{2} - \frac{1}{3} = \frac{9-2}{6} = \frac{7}{6}$$

$$f\left(\frac{14}{39} + \frac{18}{39} i\right) = \frac{1}{39} \begin{bmatrix} 14 & 18 \\ -18 & 39 \end{bmatrix} \quad \checkmark$$

$\mathbb{Q}[\sqrt{2}] \cong K = \left\{ \begin{bmatrix} a & b \\ 2b & a \end{bmatrix} : a, b \in \mathbb{Q} \right\}$ basis for K: I, $J = \begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}$, $J^2 = \begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = 2I$.

$\det \begin{bmatrix} a & b \\ 2b & a \end{bmatrix} = a^2 - 2b^2 \neq 0$ if $a, b \in \mathbb{Q}$ are not both zero.

$$\begin{bmatrix} a & b \\ 2b & a \end{bmatrix}^{-1} = \frac{1}{a^2 - 2b^2} \begin{bmatrix} a & -b \\ -2b & a \end{bmatrix}$$

Note: $\left\{ \begin{bmatrix} a & b \\ 2b & a \end{bmatrix} : a, b \in \mathbb{R} \right\}$ is a commutative ring with identity having zero divisors

$$\begin{bmatrix} \sqrt{2} & 1 \\ 2 & \sqrt{2} \end{bmatrix} \begin{bmatrix} -\sqrt{2} & 1 \\ 2 & -\sqrt{2} \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} a & b \\ 2b & a \end{bmatrix} = aI + bJ, \quad J = \begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}, \quad J^2 = \begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = 2I$$

$\alpha = \sqrt[3]{2} = 2^{1/3}$ $\quad$ $1, \alpha, \alpha^2$ is a basis: every element of $\mathbb{Q}[\alpha]$ is uniquely expressible as a linear combination $a \cdot 1 + b \cdot \alpha + c \cdot \alpha^2$, $a, b, c \in \mathbb{Q}$

$$\mathbb{Q}[\alpha] = \{a + b\alpha + c\alpha^2 : a, b, c \in \mathbb{Q}\}$$
(field)

Compare $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$
(field)

$\alpha^3 = 2$

$\alpha^3 = 2$
$\alpha^4 = 2\alpha$
$\alpha^5 = 2\alpha^2$
$\alpha^6 = 4$

$\mathbb{Q}[\alpha]$ is a 3-dimensional vector space over the scalars $a, b, c \in \mathbb{Q}$

If $E \supseteq F$ is a field extension (F is a subfield of E

$u = 2 + \alpha + \alpha^2$
$v = 1 - \alpha + \alpha^2$

$u + v = 3 + 2\alpha^2$
$u - v = 1 + 2\alpha$
$uv = (2 + \alpha + \alpha^2)(1 - \alpha + \alpha^2) = 2 - \alpha + 2\alpha^2 + \alpha^4 = 2 - \alpha + 2\alpha^2 + 2\alpha = 2 + \alpha + 2\alpha^2$

$$\frac{u}{v} = \frac{2 + \alpha + \alpha^2}{1 - \alpha + \alpha^2} = a + b\alpha + c\alpha^2 \Rightarrow 2 + \alpha + \alpha^2 = (1 - \alpha + \alpha^2)(a + b\alpha + c\alpha^2)$$

rational numbers

$$= a + (b-a)\alpha + (a-b+c)\alpha^2 + (b-c)\alpha^3 + c\alpha^4$$
$$= a + (b-a)\alpha + (a-b+c)\alpha^2 + 2(b-c) + 2c\alpha$$
$$= (a+2b-2c) + (-a+b+2c)\alpha + (a-b+c)\alpha^2$$

$a + 2b - 2c = 2$
$-a + b + 2c = 1$
$a - b + c = 1$

$$\left[\begin{array}{ccc|c} 1 & 2 & -2 & 2 \\ -1 & 1 & 2 & 1 \\ 1 & -1 & 1 & 1 \end{array}\right] \sim \left[\begin{array}{ccc|c} 1 & 2 & -2 & 2 \\ 0 & 3 & 0 & 3 \\ 1 & -1 & 1 & 1 \end{array}\right] \sim \left[\begin{array}{ccc|c} 1 & 2 & -2 & 2 \\ 0 & 1 & 0 & 1 \\ 1 & -1 & 1 & 1 \end{array}\right] \sim \left[\begin{array}{ccc|c} 1 & 2 & -2 & 2 \\ 0 & 1 & 0 & 1 \\ 0 & -3 & 3 & -1 \end{array}\right] \sim \left[\begin{array}{ccc|c} 1 & 0 & -2 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & -3 & 3 & -1 \end{array}\right] \sim \left[\begin{array}{ccc|c} 1 & 0 & -2 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 3 & 2 \end{array}\right]$$

$$\sim \left[\begin{array}{ccc|c} 1 & 0 & -2 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 2/3 \end{array}\right] \sim \begin{array}{ccccc} a & b & c & & \\ \hline 1 & 0 & 0 & 4/3 & \leftarrow a \\ 0 & 1 & 0 & 1 & \leftarrow b \\ 0 & 0 & 1 & 2/3 & \leftarrow c \end{array}$$

$\frac{u}{v} = \frac{4}{3} + \alpha + \frac{2}{3}\alpha^2$ ✓

$3.65152175(2)$

A good way to check!

Check: $\alpha \approx 1.25992104989$
$u \approx 4.84732210186$
$v \approx 1.32748000207$

$\frac{u}{v} \approx 3.651521752$

$\mathbb{Q}[\alpha] \cong \{ aI + bA + cA^2 : a,b,c \in \mathbb{Q} \} = \left\{ \begin{bmatrix} a & 2c & 2b \\ b & a & 2c \\ c & b & a \end{bmatrix} : a,b,c \in \mathbb{Q} \right\} = \mathbb{Q}[A]$

$\alpha = 2^{1/3}$

$A = \begin{bmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$

$A^2 = \begin{bmatrix} 0 & 2 & 0 \\ 0 & 0 & 2 \\ 1 & 0 & 0 \end{bmatrix}$

$A^3 = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix} = 2I$

$A^4 = 2A$

An isomorphism $f: \mathbb{Q}[\alpha] \longrightarrow \mathbb{Q}[A]$ is given by $f(a+b\alpha+c\alpha^2) = aI + bA + cA^2$

eg. $f(u) = f(2+\alpha+\alpha^2) = 2I + A + A^2 = \begin{bmatrix} 2 & 2 & 2 \\ 1 & 2 & 2 \\ 1 & 1 & 2 \end{bmatrix}$

$f(v) = f(1-\alpha+\alpha^2) = I - A + A^2 = \begin{bmatrix} 1 & 2 & -2 \\ -1 & 1 & 2 \\ 1 & -1 & 1 \end{bmatrix}$

$f(uv) = f(u)f(v) = \begin{bmatrix} 2 & 2 & 2 \\ 1 & 2 & 2 \\ 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 & -2 \\ -1 & 1 & 2 \\ 1 & -1 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 4 & 2 \\ 1 & 2 & 4 \\ 2 & 1 & 2 \end{bmatrix} = 2 + A + 2A^2$

$f\left(\frac{u}{v}\right) = f(u) f(v^{-1}) = \begin{bmatrix} 2 & 2 & 2 \\ 1 & 2 & 2 \\ 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 & -2 \\ -1 & 1 & 2 \\ 1 & -1 & 1 \end{bmatrix}^{-1}$

$\mathbb{C} \supset \mathbb{R}$ is a field extension

$\mathbb{C} = \mathbb{R}[i] = \{ a + bi : a,b \in \mathbb{R} \}$ has basis $\{1, i\}$ over $\mathbb{R}$

$\mathbb{R} \supset \mathbb{Q}$ $\quad 1, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{7}, \sqrt{10}, \ldots$

$\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$

Consider the prime field $\mathbb{F}_{101} = \{0, 1, 2, \dots, 100\}$ with $\alpha = 89$, $\beta = 23$. (Addition, multiplication, etc. mod 101)

101 is prime

$\alpha + \beta = 112 = 11$

$\alpha - \beta = 66$

$\alpha\beta = 2047 = 27$

$\frac{\beta}{\alpha} =$

$\square \times \alpha = \beta$?

$\square \cdot \alpha = 1$?

How do we compute inverses in $\mathbb{F}_p = \{0, 1, 2, \dots, p-1\}$, p prime?

Review: basic properties of $\mathbb{Z}$ (handout on website)

$\gcd(89, 101) = 1$

89 has (positive) divisors 1, 89

101 has (positive) divisors 1, 101

the only common number is 1 (common divisor of 89 and 101)

$\gcd(\overset{3\cdot 5}{15}, \overset{3\cdot 7}{21}) = 3.$

Divisors of 15: $-15, -5, -3, -1, 1, 3, 5, 15$

Divisors of 21: $-21, -7, -3, -1, 1, 3, 7, 21$

Common divisors of 15 and 21: $-3, -1, 1, 3$

greatest common divisor of 15 and 21: 3.

If $b = ra$ $(a, b, r \in \mathbb{Z})$ then we say

- a divides b
- a is a divisor of b
- b is a multiple of a
- a is a factor of b
- $a \mid b$

vertical bar

$3 \mid 15$ $\quad$ $7 \nmid 15$ $\quad$ 7 does not divide 15

$3 < 5$ $\quad$ $8 \not< 5$

$0 \mid 0$

$0 = -17 \cdot 0$

Divisors of 1: $-1, 1$

Divisors of 0: $\dots, -3, -2, -1, 0, 1, 2, 3, \dots$

$3 \mid 0$ because $0 = 0 \cdot 3$

Fact: Given $a, b \in \mathbb{Z}$, not both zero, $\gcd(a,b) = r \cdot a + s \cdot b$ for some $r, s \in \mathbb{Z}$.
We can "easily" compute $\gcd(a,b)$, r, s, using the extended Euclidean algorithm.

eg. $\gcd(89, 101) = \boxed{} = \boxed{42} \cdot 89 + \boxed{-37} \cdot 101.$

$$101 = 1 \times 89 + 12$$
$$89 = 7 \times 12 + 5$$
$$12 = 2 \times 5 + 2$$
$$5 = 2 \times 2 + \boxed{1} \leftarrow \gcd(101, 89) = 1$$
$$2 = 2 \times 1 + 0$$

$$\begin{aligned}
1 &= 5 - 2 \times 2 \\
&= 5 - 2 \times (12 - 2 \times 5) \\
&= 5 \times 5 - 2 \times 12 \\
&= 5 \times (89 - 7 \times 12) - 2 \times 12 \\
&= 5 \times 89 - 37 \times 12 \\
&= 5 \times 89 - 37 \times (101 - 89) \\
&= 42 \times 89 - 37 \times 101
\end{aligned}$$

$$21 = 1 \times 15 + 6$$
$$15 = 2 \times 6 + \boxed{3} \leftarrow \gcd(21, 15) = 3$$
$$6 = 2 \times 3 + 0$$

$3 = \boxed{-2} \times 21 + \boxed{3} \times 15$?

$$\begin{aligned}
3 &= 15 - 2 \times 6 \\
&= 15 - 2 \times (21 - 15) \\
&= 3 \times 15 - 2 \times 21
\end{aligned}$$

Check: $45 - 42 = 3$.