1 a левый делитель (делит слева) b: $b = ac$. В коммутативных — просто делитель. Всё транзитивно. Если есть единица — рефлексивно. Коммутативное с единицей — область целостности, есть нет делителей нуля ($\neq 0$).

2 В любом кольце. Левый идеал: складываем/вычитаем и $a \in I \Rightarrow xa \in I$. Двухсторонний идеал: вычитаем и умножаем с любой стороны. Можно пересекать, складывать (суммы элементов), умножать (произведения элементов, если один был левый, другой правый $\Rightarrow$ двухсторонний).

3 Порождается X, если наименьший по включению, содержащий X. Обозначается $I = (a_1, a_2, \ldots, a_n)$. Или если равен множеству линейных комбинаций. Главный, если порождается одним элементом. $a \mid b \Rightarrow$ один идеал вложен в другой. Область главных идеалов (ОГИ), если все главные. Контрпример: $\mathbb{R}[x, y]$

4 Мультипликативная группа $R*$ из обратимых элементов ($ab = ba = 1$). Ассоциированность: есть $x \in R*$ такой, что $a = bx$. Отношение эквивалентности. $a \sim b \Rightarrow a \mid b \wedge b|a$, в обратную в области целостности.

5 НОД, если делитель всех и делится на любой с таким же свойством. В области целостности определён с точностью до ассоциированности. Взаимная простота, если НОД — единица. Если НОД, то разделим, получим взаимно простые (нужна единица). Если идеал, порождённый X равен (d), то это НОД и есть линейное представление. В ОГИ для любых есть НОД и линейное представление, а также свойство про идеалы. В $\mathbb{R}[x, y]$ линейное представление не всегда есть. В ОГИ если $a \mid bc$, то при взаимной простоте $\Rightarrow a \mid c$ (выразили c по линейности через a, b).

6 R — область целостности. Евклидова норма из $R \setminus \{0\}$ в $\mathbb{N}$, если можно делить с остатком (у остатка маленькая норма). Евклидово кольцо, если можно задать норму. Пример: целые ($|x|$), гауссовы ($a^2 + b^2$, поделили x на y просто так, домножив на сопряжённое, округлили, сказали, что это частное, оценили).

7 Строим последовательность $r = ax + by$, делим с остатком r_{i-1} на r_i, получаем следующую строчку. Норма r_i уменьшается, она натуральна, когда-нибудь получим ноль (не имеющий нормы). Раскрутили обратно, получили линейное представление.

8 Разобрали (0) отдельно. Теперь взяли элемент b с наименьшей нормой (кроме нуля). Очевидно, что $(b) \subseteq I$. Взяли элемент из $I \setminus (b)$, поделили с остатком на b, противоречие.

9 Классификация всего, кроме нуля и $R*$ (коммутативная группа). Составной, если $a = bc$, где $b, c \notin R*$. Неприводимый, если $a = bc \Rightarrow b \in R * \vee c \in R*$. Простой, если $a \mid bc \Rightarrow a \mid b \vee a \mid c$. Если область целостности, то всякий простой неприводим (если $p = bc$, то либо $p \sim b$, либо $p \sim c$).

10 В ОГИ любой неприводимый прост. Если $p \mid ab$, то либо $p \mid a$, либо нет. Тогда рассмотрим (p, a), в ОГИ это (d). Значит $p = dv$, отсюда $d \in R*$ (если $v \in R*$, то $p \sim d$ и $p \mid a$). То есть $(p, a) = (d) = (1)$, то есть p и a взаимно просты. Значит, $p \mid ab \Rightarrow p \mid b$.

11 Факториально, если разложили на мультимножество простых с точностью до порядка и домножение на элемент $R*$. Не факториально $\mathbb{Z}[\sqrt{-5}]$: $6 = 2 \cdot 3 = (1 + \sqrt{5}i)(1 - \sqrt{5}i)$ (ввели норму $a + 5b^2$, мультипликативна, нашли $R*$. нашли все элементы маленькой нормы).

12 Нётерово кольцо — нет бесконечной строгой цепочки идеалов. Равносильно тому, что все идеалы конечнопорождены. Если R — ОГИ (и тогда Нётерово), то оно факториально. Сначала покажем, что всегда существует неприводимый делитель. Будем a и раскладывать на составные, получим бесконечную цепочку, упс. Теперь разложим: будем делить; если до бесконечности, то возьмём произведения на суффиксах и получим бесконечную цепочку, упс. Единственность: пусть есть два разложения, одно короче другого, индукция по длине кратчайшего. Возьмём простое из первого, найдём, кого из второго разложения оно делит, сократим.

13 Если K — поле, то в $K[x]$, линейный неприводим. Если K алгебраически замкнуто, то по Безу других неприводимых нет. $\mathbb{C}$ — такое (без доказательства). Замечание: если степень 2 или 3, то неприводимость $\iff$ отсутствие корней (посмотрели на степени делителей). Теперь к $\mathbb{R}$, покажем, что можно разложить на степени не больше 2 (если степень 2, то отрицательный дискриминант). Разложим над $\mathbb{C}$, если z — корень, то $\bar{z}$ тоже корень, причём той же кратности (это через производные), объединим их по парам.

14 $a \equiv b(\mod I) \iff (a - b) \in I$. Рефлексивно, симметрично, транзитивно. Можно ввести классы эквивалентности, независимо от представителей всё будет ок.

15 R/I — факторкольцо, надо еще раз проверить корректность операций и всякие свойства колец. Если было коммутативным/с единицей, то фактор тоже коммутативно/с единицей.

16 Идеал максимальный, если любой его содержащий равен либо ему, либо кольцу (максимальный по включению, может быть много). I — максимальный $\iff$ R/I — поле. $\Rightarrow$: единица в факторкольце лежит и не равна нулю (потому что $I \subsetneq R$), докажем существование обратного: взяли элемент a, взяли идеал $I + (a)$ (получили R по максимальности), в нём нашли единицу вида $1 = x + ab$ (где $x \in I$, $b \in R$), это есть обратный. $\Leftarrow$: от противного, пусть есть $I \subsetneq J$ (тоже идеал), покажем $J = R$. Взяли $a \in J \setminus I$, взяли обратный в поле b, получили $1 \equiv ab(\mod I)$. Так как J — идеал, то $ab \in J$, $c \in I \subset J \Rightarrow ab + c \in J \Rightarrow 1 \in J \Rightarrow J = R$. Еще теорема в ОГИ: (a) — максимальный $\iff$ a неприводим, док-во: разложили на неприводимые (они же в ОГИ простые). Следствия: $\mathbb{Z}/m\mathbb{Z}$ иногда поле, $K[x]/f$ иногда поле.

17 Вычеты по модулю $x^2 + 1$ в $\mathbb{R}[x]$.

18 Взяли неприводимый в $F[x]$ многочлен f степени n, взяли факторкольцо $K = F[x]/(f)$, тогда оно поле. Рассмотрим естественный гомоморфизм из кольца в поле (по модулю идеала; надо что-то сказать про инъективность констант), возьмём $[x]$, он является корнем f, так как $f([x]) = [0]$. K — это поле, полученное присоединением корня f. Возьмём другой многочлен g (хотя бы степени 1) над $F[x]$, где F — поле. Поле K есть поле разложения f, если в K он раскладывается на линейные, а в любом подполе — нет. Теорема: для любого f существует такое поле. Для начала найдём какое нибудь (не обязательно минимальное). Просто делаем индукцию по суммарной степени нелинейный множителей, берём какой-нибудь множитель, присоединяем корень, расширяем поле. Дальше можно просто пересечь все подполя результата, в которых разложим f, потому что все корни в поле мы знаем — их ровно n, новым взяться неоткуда.

19 Пусть R — область целостности, хотим построить поле $F \supset R$. Введём множество дробей (знаменатель не ноль), отношение эквивалентности на них, возьмём фактор. Покажем, что операции корректны, что это поле, что $\frac{a}{1}$ изоморфно R.

20 Поле частных $F[x]$ (F — поле) есть поле рациональных функций. Покажем, что всякая дробь единственным образом записывается в виде $\frac{f}{g}$, старший коэффициент в g единица, НОД тоже единица (почему-то это было определением **TODO**). Дробь правильная, если числитель меньше знаменателя. Примарная, если $g = q^k$, q неприводим, $\deg f < \deg g$. Простейшая, если $g = q^k$, $\deg f < \deg q$. Теорема: единственно разложение в сумму простейших и многочлена (он не простейшая). План: сначала разложим в многочлен и правильную (поделили с остатком), потом правильную в примарные, потом примарные в простейшие. Лемма: правильную $\frac{f}{gh}$ можно разложить в правильные $\frac{f}{g} + \frac{f}{h}$ (при НОД=1). Для этого (так как F — ОГИ) представили НОД линейно, поделим переменные с остатком на знаменатели, покажем, что получили хорошие степени. Правильную в примарные: разложили знаменатель, индукция по числу множителей. Примарную в простейшие: индукция по степени q^k, на каждом шаге делим с остатком на q. Единственность: индукция по суммарному количеству простейших, на шаге домножаем на общие знаменатели и вычитаем.

21 Взяли перестановки, ввели знак перестановки (через инверсии, есть геометрический смысл «наклон отрезка между выбранными элементами»), ввели определитель.

22 Транспонирование не меняет ничего (нарисовали, что такое «наклон отрезка»), значит, строки и столбцы равноправны. Меняем соседние строки местами: геометрически поменялись только отрезки между этими строчками, сменился знак. Транспозиция строк: нечётное число транспозиций соседних (туда и обратно). Если две строки одинаковы, то переставим, знак поменялся $\Rightarrow$ ноль.

23 Миноры: вычеркнули строку и столбец, посчитали определитель. Алгебраическое дополнение: минор на знак (сумма номеров строки и столбца). Если транспонируем, алг.доп. тоже транспонируются. Если в i-й строчке все нули (кроме a_{ij}), то можно разложить по этому элементу через алгебраическое дополнение.

24 Можно разложить по строке: сумма элементов на их алг.доп. Если в разложении по строке взять алг.доп. из другой строки, будет ноль. Если строчку умножить на c, определитель умножится на c. Есть две пропорциональные строки $\Rightarrow$ ноль. Если строчку разложим на сумму двух строк, можно разложить так же определитель (из предыдущих очевидно).

25

$$\begin{vmatrix} 1 & x_1 & x_1^2 & \dots x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots x_2^{n-1} \\ 1 & x_3 & x_3^2 & \dots x_3^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{n-1} & x_{n-1}^2 & \dots x_{n-1}^{n-1} \end{vmatrix} = \prod_{i>j}(x_i - x_j)$$

Занунили последнюю строчку, разложили по ней, вынесли множители $\prod(x_i - x_n)$, получили рекурсию.

26

$$\begin{vmatrix} A_1 & 0 \\ B & A_2 \end{vmatrix} = |A_1| \cdot |A_2|$$

Индукция по порядку матрицы A_1. Можно обобщить на матрицу из нескольких диагональных клеток.

27 Крамер: заменили i-й столбец в матрице системы столбцом свободных, посчитали определитель, поделили на определитель системы. Теорема: если определитель системы не ноль, есть ровно одно решение, по формулам. Сначала докажем единственность: домножим строчки на алгебраические дополнения первого столбца, получим формулу для x_1, аналогично для x_k. Корректность «в лоб».

28 Вводим минор порядка k для прямоугольной матрицы (выбрали какие-то k строк/столбцов, считаем определитель). Если все миноры порядка k нули, то и большего порядка тоже нули. Ранг: максимальный порядок минора такой, что есть ненулевой. Если везде нули, то ранг ноль.

29 Можно умножать строчку на число, прибавлять другую строчку с коэффициентом, переставлять строки местами (и со столбцами то же). Это обратимо и перестановка выражается через первые два. В лоб можно показать, что при преобразованиях ранг не меняется (так как занулённость миноров получается равносильной). Можно привести к трапецевидной (сначала на диагонали единицы, а ниже нули). Если приписываем нулевую строчку, ранг сохраняется. Если приписываем какую-то строчку, ранг увеличивается не больше, чем на единицу.

30 Записали прямоугольную матрицу системы и расширенную матрицу (приписали справа свободные члены). Пусть ранги r_A и r_B. Теорема: совместность системы (существование решения) $\iff$ $r_A = r_B$. $\Rightarrow$: сделали в матрице B новый столбец нулём элементарными преобразованиями, ой, отличаются только столбцом нулей. $\Leftarrow$: возьмём r_A уравнений, покажем равносильность существования их решения чему надо. Если существует решение большей, то оно же и для меньшей. В другую сторону: занулим в расширенной матрице первые r_A строк последнего столбца, ранг сохранился. Значит, любой минор порядка $r_A + 1$ нулевой, возьмём такой: первые r_A строк и любая, разложим по последнему столбцу. Теперь покажем, что у меньшей системы есть решение. Если $r_A = n$, то квадратная матрица и всё ок. Если $r_A < n$, то придадим последним любые значения, остальные выразятся. Доказали. Отсюда следствие про однородные системы: чтобы было нетривиальное решение, надо маленький ранг (т.е. нулевой определитель)

31

$$\begin{vmatrix} A & 0 \\ -E & B \end{vmatrix} = |A| \cdot |B|$$

Преобразуем левую часть так, чтобы кусок B занулился, над ним получим матрицу C, у неё определитель равен определителю C. Теперь посмотрим на C и увидим, что оно в точности по формуле перемножения.

32 Обратна матрица обратна с двух сторон (потом увидим, что односторонних не бывает). Взаимная матрица — заменили элементы на алг.доп. и потом транспонировали. В лоб покажем, что $A\tilde{A} = \tilde{A}A = |A| \cdot E$. Поделим, видимо, что если определитель не ноль (матрица неособенная), то есть решение, причём двухстороннее. Отсюда следует единственность.

33 $AX = \lambda X$ — собственное число и вектор-столбец. Сделали соответствующую систему матрицы однородной, обозначили λ переменной, приравняли определитель нулю (хотим нетривиальное решение). Получили характеристический многочлен степени n (надо показать, что старший коэффициент не ноль).

34 По построению из предыдущего. Для поиска векторов надо решать систему.

35 Взяли характеристический многочлен $\phi(t)$, подставили вместо t матрицу A (умножать-то умеем), посчитали, получили, внезапно, ноль. Док-во: давайте разрешим класть в ячейки не только числа, но и многочлены. Потом рассмотрим матрицу $B(t) = A - Et$, по определению $|B| = \phi$. Пусть $\phi(t) = a_0 + a_1 t + \cdots + a_n t^n$. Составим $\tilde{B} = B_0 + B_1 t + B_2 t^2 + \cdots + B_{n-1} t^{n-1}$ (степени не больше $n-1$, так как исходно всё линейно, а миноры есть произведения $n-1$ члена). Теперь помним, что $B\tilde{B} = \Delta E = \phi(t)E$. Получили систему $AB_0 = a_0 E; AB_1 - B_0 = a_1 E; AB_2 - B_1 = a_2 E; \ldots$. Домножили на степени A, сложили. Слева занулится, справа получим $\phi(A)$.