Лекция №7

Тема: Квадратичное расширение. Разрешимость уравнения третьей степени в квадратных радикалах

План лекции:

1. Понятие квадратичного расширения
2. Основная теорема о квадратичном расширении
3. Теорема о разрешимости кубического уравнения в квадратных радикалах

Литература:

1.Окунев Л. Я. Высшая алгебра. – М.: Изд-во «Просвещение», 1966. – 336. (Параграфы 19-20).

Текст лекции

Как известно, многие геометрические задачи на построение можно свести к нахождению корней алгебраического уравнения

$$a_0x^n + a_1x^{n-1} + \ldots + a_n = 0 \qquad (1)$$

n-й степени, коэффициенты которого, вообще говоря, комплексные. Например, задача об удвоении куба тесно связана с извлечением корня третьей степени из 2, задача трисекции угла — с неприводимым случаем неполного кубического уравнения.

В курсе теории геометрических построений доказывается, что некоторое выражение α тогда и только тогда может быть построено при помощи циркуля и линейки, когда оно получается в результате решения уравнений не выше второй степени. Например, выражение

$$\alpha = \sqrt[4]{1+\sqrt{2}}$$

можно построить при помощи циркуля и линейки, так как оно получается в результате решения ряда уравнений не выше второй степени, а именно: $\alpha_1 = \sqrt{2}$ есть корень квадратного уравнения $x^2 - 2 = 0$, и мы можем построить $\sqrt{2}$ при помощи циркуля и линейки. Далее, $\alpha_2 = 1 + \sqrt{2}$ является корнем уравнения первой степени $x - (1 + \alpha_1) = 0$, и мы можем $1 + \sqrt{2}$ также построить при помощи циркуля и линейки, — придется складывать отрезки, соответствующие 1 и $\sqrt{2}$. Затем $\alpha_3 = \sqrt{\alpha_2}$ является корнем квадратного уравнения $x^2 - \alpha_2 = 0$, и, поскольку α_2 было уже заранее построено, мы этот корень без труда построим при помощи циркуля и линейки. Наконец, $\alpha = \sqrt{\alpha_3}$ есть корень квадратного уравнения $x^2 - \alpha_3 = 0$, а так как α_3 уже построено, то мы построим при помощи циркуля и линейки и $\alpha = \sqrt{\alpha_3}$.

Таким образом, если α — корень алгебраического уравнения 1), то этот корень может быть построен при помощи циркуля и линейки в том и только в том случае, когда он выражается через квадратные радикалы.

Возникает естественный вопрос: при каких условиях, необходимых и достаточных, уравнение (1) степени $n \geqslant 3$ решается в квадратных радикалах? Мы ограничимся тем, что дадим исчерпывающий ответ для случая уравнения третьей степени с комплексными коэффициентами.

Введем для этой цели понятие квадратичного расширения числового поля. Пусть P — некоторое числовое поле и α — корень квадратного многочлена $p(x)$, неприводимого над P. Очевидно, что число α не содержится в поле P; в противном случае многочлен $p(x)$ оказался бы приводимым над P. Без ограничения общности выводов можно предположить, что старший коэффициент многочлена $p(x)$ равен единице: $p(x) = x^2 + px + q$, где p, q — числа из P; в противном случае мы разделили бы многочлен $P(x)$ на его старший коэффициент. Обозначим теперь через $P(\alpha)$ (α в круглых скобках!) множество чисел, которые могут быть получены с помощью конечной комбинации арифметических действий сложения, вычитания и умножения, производимых над α и над числами из поля P, т. е. множество чисел вида

$$\omega = f(\alpha) = c_0 + c_1\alpha + \ldots + c_k\alpha^k, \qquad (2)$$

где k — произвольное целое неотрицательное число, $c_0, c_1, \ldots, c_k$ — любые числа из поля[1] P. Мы собираемся доказать следующую теорему.

Теорема. *Множество $P(\alpha)$ является числовым полем.*

Доказательство. Легко видеть, что $P(\alpha)$ есть числовое кольцо: складывая, вычитая, перемножая числа вида (2), мы получаем числа того же вида. Остается убедиться, что частное $\frac{\omega_1}{\omega_2}$ чисел ω_1 и $\omega_2 \neq 0$ множества $P(\alpha)$ принадлежит тому же множеству.

Покажем предварительно, что всякое число $\omega = c_0 + c_1\alpha + \ldots + c_k\alpha^k$ из $P(\alpha)$ представимо в виде двучлена $a + b\alpha$, где a и b — числа из P.

В самом деле, обозначим через $q(x)$ частное, $r(x)$ — остаток при делении многочлена $f(x) = c_0 + c_1 x + \ldots + c_k x^k$ на $p(x)$. Так как степень остатка должна быть ниже степени 2 делителя, то мы можем положить $r(x) = a + bx$, где a, b — некоторые числа из поля P. Таким образом, $f(x) = p(x) \cdot q(x) + (a + bx)$. Полагая в этом равенстве $x = \alpha$, получаем $\omega = f(\alpha) = a + b\alpha$, так как $p(\alpha) = 0$. Очевидно, что, обратно, двучлен вида $a + b\alpha$, где a, b — числа из P, есть число из $P(\alpha)$.

[1] Если бы многочлен $p(x)$ был приводим над P или, что то же, α принадлежало бы P, то множество $P(\alpha)$ совпадало бы с P.

Пусть теперь $\omega_1 = a_1 + b_1\alpha$ и $\omega_2 = a_2 + b_2\alpha \neq 0$ — два каких-нибудь числа из множества $P(\alpha)$. Рассмотрим их частное:

$$\frac{\omega_1}{\omega_2} = \frac{a_1 + b_1\alpha}{a_2 + b_2\alpha}.$$

Избавимся от «иррациональности» в знаменателе, для чего умножим числитель и знаменатель на $a_2 + b_2\beta$, где β — второй корень многочлена $p(x)$; $a_2 + b_2\beta \neq 0$, ибо β не принадлежит P. Получаем:

$$\frac{\omega_1}{\omega_2} = \frac{(a_1 + b_1\alpha)(a_2 + b_2\beta)}{(a_2 + b_2\alpha)(a_2 + b_2\beta)} = \frac{a_1a_2 + a_2b_1\alpha + a_1b_2\beta + b_1b_2\alpha\beta}{a_2^2 + a_2b_2(\alpha + \beta) + b_2^2\alpha\beta}.$$

По формулам Виета $\alpha + \beta = -p$, $\alpha\beta = q$. Следовательно,

$$\frac{\omega_1}{\omega_2} = \frac{(a_1a_2 + qb_1b_2) + a_2b_1\alpha + a_1b_2(-p - \alpha)}{a_2^2 + qb_2^2 - pa_2b_2} = a + b\alpha,$$

где

$$a = \frac{a_1a_2 + qb_1b_2 - pa_1b_2}{a_2^2 + qb_2^2 - pa_2b_2}, \qquad b = \frac{a_2b_1 - a_1b_2}{a_2^2 + qb_2^2 - pa_2b_2}$$

есть числа из поля P. Мы видим, что частное $\frac{\omega_1}{\omega_2}$ также принадлежит множеству $P(\alpha)$, и теорема доказана.

Поле $P(\alpha)$ является расширением P, так как $\omega = a + b\alpha$ при $b = 0$ превращается в число $\omega = a$ из P. Мы будем $P(\alpha)$ называть *квадратичным расширением поля P, получающимся путем присоединения к P числа α*. При этом переход от поля P к полю $P(\alpha)$ будет называться *присоединением* числа α к P.

Возьмем теперь несколько комплексных чисел $\alpha_1, \alpha_2, \ldots, \alpha_s$, где α_1 — корень квадратного многочлена $p_1(x)$, неприводимого над P, α_2 — корень квадратного многочлена $p_2(x)$, неприводимого над $P_1 = P(\alpha_1)$, α_3 — корень квадратного многочлена $P_3(x)$, неприводимого над $P_2 = P_1(\alpha_2)$, $\ldots$, α_s — корень квадратного многочлена $P_s(x)$, неприводимого над $P_{s-1} = P_{s-2}(\alpha_{s-1})$. Присоединим сначала к P число α_1. Получим квадратичное расширение $P(\alpha_1)$. Затем присоединим к $P_1 = P(\alpha_1)$ число α_2. Получится дальнейшее квадратичное расширение, которое мы обозначим через $P(\alpha_1, \alpha_2)$ и т. д. После всех таких последовательных присоединений чисел $\alpha_1, \alpha_2, \ldots, \alpha_s$ мы придем к расширению $P(\alpha_1, \alpha_2, \ldots, \alpha_s)$ поля P. Мы будем называть $P(\alpha_1, \alpha_2, \ldots, \alpha_s)$ *расширением поля P, полученным путем присоединения к P чисел $\alpha_1, \alpha_2, \ldots, \alpha_s$*.

Легко видеть, что расширение $P(\alpha_1, \alpha_2, \ldots, \alpha_s)$ исчерпывается числами вида:

$$A_1\alpha_1^{k_1}\alpha_2^{k_2}\ldots\alpha_s^{k_s} + \ldots + A_p\alpha_1^{t_1}\alpha_2^{t_2}\ldots\alpha_s^{t_s},$$

где $A_1, \ldots, A_p$ — числа из P и $k_i, \ldots, t_j$ — целые неотрицательные числа, т. е. числами, получающимися из $\alpha_1, \alpha_2, \ldots, \alpha_s$ и из чисел по-

ля P в результате конечной комбинации первых трех арифметических действий.

Введем еще одно важное понятие. Обозначим через Δ множество чисел, получающихся из коэффициентов $a_0, a_1, \ldots, a_n$ уравнения (1) и из рациональных чисел с помощью конечной комбинации арифметических действий сложения, вычитания, умножения и деления (исключая деление на нуль). Иными словами, Δ есть не что иное, как множество чисел вида

$$\frac{A_1 a_0^{k_0} a_1^{k_1} \ldots a_n^{k_n} + \ldots + A_r a_0^{s_0} a_1^{s_1} \ldots a_n^{s_n}}{B_1 a_0^{l_0} a_1^{l_1} \ldots a_n^{l_n} + \ldots + B_q a_0^{p_0} a_1^{p_1} \ldots a_n^{p_n}},$$

где A_i, B_j — рациональные числа, а $k_i, \ldots, s_i, l_i, \ldots, p_i$ — целые неотрицательные числа (знаменатель, конечно, отличен от нуля). Нетрудно убедиться, что множество Δ есть числовое поле. Это поле Δ будет в дальнейшем называться *областью рациональности* уравнения (1) или многочлена $f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n$.

Теперь мы можем сказать, что *корень x_0 уравнения (1) тогда и только тогда выражается через квадратные радикалы* $\rho_1 = \sqrt{A_1}$, $\rho_2 = \sqrt{A_2}, \ldots, \rho_k = \sqrt{A_k}$, *где* A_1 *— число, принадлежащее области рациональности* Δ, A_2 *— число, принадлежащее* $\Delta(\rho_1)$, A_3 *— число, принадлежащее* $\Delta(\rho_1, \rho_2)$, *и т. д.,* A_k *— число, принадлежащее* $\Delta(\rho_1, \rho_2, \ldots, \rho_{k-1})$, *если этот корень содержится в расширении* $\Delta(\rho_1, \rho_2, \ldots, \rho_k)$.

В самом деле, если x_0 получается из радикалов $\rho_1, \rho_2, \ldots, \rho_k$, из коэффициентов уравнения (1) и некоторой системы рациональных чисел с помощью конечной комбинации четырех арифметических действий, то x_0 содержится в $\Delta(\rho_1, \rho_2, \ldots, \rho_k)$, так как $\Delta(\rho_1, \rho_2, \ldots, \ldots, \rho_k)$ есть числовое поле, содержащее область рациональности Δ и радикалы $\rho_1, \rho_2, \ldots, \rho_k$. Обратно, если x_0 содержится в $\Delta(\rho_1, \rho_2, \ldots, \rho_k)$, то x_0 получается из радикалов $\rho_1, \rho_2, \ldots, \rho_k$, коэффициентов уравнения (1) и из некоторой системы рациональных чисел с помощью конечной комбинации четырех арифметических действий.

Применим полученные результаты к проблеме разрешимости уравнения третьей степени с комплексными коэффициентами:

$$f(x) = x^3 + a_1 x^2 + a_2 x + a_3 = 0 \qquad (1)$$

Пусть какой-нибудь корень x_1 уравнения (1) выражается через квадратные радикалы

$\rho_1 = \sqrt{A_1}$, $\rho_2 = \sqrt{A_2}, \ldots, \rho_k = \sqrt{A_k}$, где k$\gg 1$

и A_1 — элемент области рациональности P уравнения (1), A_2 — элемент поля $P(\rho_1)$, A_3 — элемент поля $P(\rho_1, \rho_2)$ и т. д., наконец, A_k — элемент поля $P(\rho_1, \rho_2, \ldots, \rho_{k-1})$. Посмотрим, что можно получить относительно остальных корней x_2 и x_3 уравнения (1).

Так как x_1 — корень многочлена $f(x) = x^3 + a_1x^2 + a_2x + a_3$, то $f(x) = (x - x_1)(x^2 + px + q)$. Пользуясь схемой Горнера, без труда находим, что $p = x_1 + a_1$, $q = x_1^2 + a_1x_1 + a_2$. Далее, очевидно, что x_2 и x_3 должны быть корнями уравнения

$$x^2 + px + q = 0.$$

Следовательно, по формуле решения квадратного уравнения

$$x_2 = -\frac{p}{2} + \rho_{k+1}, \qquad x_3 = -\frac{p}{2} - \rho_{k+1},$$

где ρ_{k+1} — одно из значений $\sqrt{\frac{p^2}{4} - q}$. Мы видим отсюда, что x_2 и x_3 выражаются через p и ρ_{k+1}, величины p и q выражаются через a_1, a_2, и x_1, а x_1 выражается через квадратные радикалы ρ_1, ρ_2, ..., ρ_k. Значит, x_2 и x_3 выражаются через квадратные радикалы $\rho_1, \rho_2, \ldots, \rho_{k+1}$.

Итак, *если по меньшей мере один корень уравнения* (1) *выражается через квадратные радикалы, то уравнение разрешимо в квадратных радикалах, т. е. его остальные корни также выражаются через квадратные радикалы.*

Когда же уравнение (1) разрешимо в квадратных радикалах? Ответ дает следующая теорема.

Теорема (о разрешимости кубического уравнения в квадратных радикалах). *Уравнение третьей степени*

$$f(x) = x^3 + a_1x^2 + a_2x + a_3 = 0 \qquad (2)$$

с комплексными коэффициентами тогда и только тогда разрешимо в квадратных радикалах, когда оно имеет в своей области рациональности P по меньшей мере один корень.

Доказательство. Если уравнение (2) имеет в области рациональности P корень a, то многочлен $f(x) = x^3 + a_1x^2 + a_2x + a_3$ распадается над полем P в произведение следующих множителей:

$$f(x) = (x - a)(x^2 + px + q).$$

Таким образом, уравнение (2) распадается над P на уравнения первой и второй степени и тем самым решается в квадратных радикалах.

Обратно, пусть уравнение (2) разрешимо в квадратных радикалах. Допустим, что при этом уравнение (2) не имеет корней в области рациональности P. Возьмем какой-нибудь корень x_1 уравне-

ния или, что то же, многочлена $f(x)$. Пусть x_1 выражается через квадратные радикалы $\rho_1 = \sqrt{A_1}, \rho_2 = \sqrt{A_2}, \ldots, \rho_k = \sqrt{A_k}$, где $k > 1$, A_1 — элемент поля P, A_2 — элемент поля $P(\rho_1)$ и т. д. Мы вправе предположить, что радикал ρ_i не лежит в $P(\rho_1, \ldots, \rho_{i-1})$ $(i = 2, \ldots, k)$ и ρ_1 не лежит в P; в противном случае он был бы лишним и его можно было бы удалить; при этом все радикалы удалить не придется: если бы оказались лишними все $\rho_1, \rho_2, \ldots, \rho_k$, то x_1 лежало бы в P, что невозможно, так как уравнение (2) не имеет корней в области рациональности P. Затем мы имеем право допустить, что x_1 не лежит в поле $P(\rho_1, \rho_2, \ldots, \rho_{k-1})$; если бы это было не так, то радикал ρ_k был бы для x_1 лишним. Таким образом, можно написать, что

$$x_1 = p + q\rho_k,$$

где p, q — элементы поля $P(\rho_1, \rho_2, \ldots, \rho_{k-1})$ и $q \neq 0$.

Несложный подсчет обнаруживает, что $x_2 = p - q\rho_k$ также является корнем многочлена $f(x)$, а именно, подставляя значение x_1 в уравнение (2), после очевидных преобразований получаем:

$$f(x_1) = R + Q\rho_k = 0,$$

где $$R = p^3 + 3pq^2A_k + a_1p^2 + a_1q^2A_k + a_2p + a_3,$$

$$Q = 3p^2q + A_kq^3 + 2a_1pq + a_2q.$$

Ясно, что R и Q являются элементами поля $P(\rho_1, \ldots, \rho_{k-1})$.

Теперь, если допустить, что $Q \neq 0$, то $\rho_k = -\frac{R}{Q}$ и радикал ρ_k лежал бы в $P(\rho_1, \ldots, \rho_{k-1})$, что невозможно. Следовательно, $Q = 0$ и тем самым $R = 0$.

Подставляя в многочлен $f(x)$ вместо x число $x_2 = p - q\rho_k$, получаем после аналогичных преобразований, что $f(x_2) = R - Q\rho_k$. Но $R = Q = 0$. Значит, $f(x_2) = 0$, т. е. x_2 также является корнем многочлена $f(x)$. При этом $x_2 \neq x_1$, так как $q \neq 0$.

Обозначим, далее, через x_3 третий корень многочлена $f(x)$. Тогда формула Виета дает:

$$x_1 + x_2 + x_3 = -a_1, \text{ откуда}$$

$$x_3 = -a_1 - x_1 - x_2,$$

или, подставляя значения x_1 и x_2:

$$x_3 = -a_1 - 2p.$$

Мы видим, что x_3 лежит в поле $P(\rho_1, \ldots, \rho_{k-1})$, так как a_1 и p лежат в $P(\rho_1, \ldots, \rho_{k-1})$.

Повторим для корня x_3 те же рассуждения, что и для x_1. Так как x_3 выражается через радикалы $\rho_1, \rho_2, \ldots, \rho_{k-1}$, то мы получим, что x_1 и x_2 лежат в $P(\rho_1, \rho_2, \ldots, \rho_{k-1})$. Но это невозможно, так как x_1 не лежит в $P(\rho_1, \rho_2, \ldots, \rho_{k-1})$.

Отметим одно следствие, вытекающее из только что доказанной теоремы.

Следствие. *Уравнение третьей степени с рациональными коэффициентами тогда и только тогда разрешимо в квадратных радикалах, когда оно имеет по меньшей мере один рациональный корень.*

В самом деле, в этом случае область рациональности P будет совпадать с полем рациональных чисел.

Рассмотрим теперь следующие задачи на геометрические построения.

Задача об удвоении куба, как известно, сводится к уравнению третьей степени

$$f(x) = x^3 - 2 = 0 \qquad (3)$$

с рациональными коэффициентами. Это уравнение, однако, не имеет рациональных корней, так как число $\sqrt[3]{2}$ иррационально. Следовательно, уравнение (3) нельзя решить в квадратных радикалах, и потому задача об удвоении куба неразрешима при помощи циркуля и линейки.

Обратимся к знаменитой задаче о трисекции угла. Она заключается в следующем: дан угол α, требуется его разделить на три равные части. Обозначим искомый угол через φ. Тогда

$$\cos\alpha = \cos 3\varphi = 4\cos^3\varphi - 3\cos\varphi.$$

Поскольку угол α дан, мы можем считать его косинус также заданным. Поэтому полагаем $\cos\alpha = \frac{b}{2}$, а $\cos\varphi$ обозначаем через $\frac{x}{2}$. Таким образом,

$$\frac{b}{2} = 4\left(\frac{x}{2}\right)^3 - 3\left(\frac{x}{2}\right),$$

или окончательно:

$$f(x) = x^3 - 3x - b = 0^1.$$

Возьмем, например, $\alpha = \frac{\pi}{3}$. В этом случае $b = 1$, и мы получаем уравнение $x^3 - 3x - 1 = 0$ с рациональными коэффициентами. Нетрудно убедиться, что это уравнение не имеет рациональных корней. Следовательно, угол $\alpha = \frac{\pi}{2}$ нельзя разделить на три равные части при помощи циркуля и линейки.