Теория Галуа, лекция 8: циклические расширения и теорема Абеля

Миша Вербицкий

15 марта, 2013

матфак ВШЭ

Расширения полей (повторение)

ОПРЕДЕЛЕНИЕ: Расширение поля k есть поле K, содержащее k.

ОПРЕДЕЛЕНИЕ: Конечное расширение есть расширение $[K : k]$ такое, что K конечномерно как векторное пространство над k. **Степень** конечного расширения есть размерность K как векторного пространства над k.

ОПРЕДЕЛЕНИЕ: Элемент K называется **алгебраическим над** k, если он содержится в конечном расширении $[K' : k]$, то есть мультипликативно порождает поле K'', конечномерное над k. **Алгебраическое расширение** есть такое расширение $[K : k]$, что все элементы K алгебраичны над k.

ТЕОРЕМА: Сумма, произведение, частное алгебраических над k **элементов алгебраично над** k**.** ■

Примитивные расширения (повторение)

УТВЕРЖДЕНИЕ: Пусть $v \in R$ – элемент конечномерной алгебры R над k, а $P(t)$ – его минимальный полином. **Тогда подалгебра $R_v \subset R$, порожденная v, изоморфна $k[t]/(P)$.**

ОПРЕДЕЛЕНИЕ: Полином $P(t) \in k[t]$ **неприводим**, если его нельзя разложить на множители положительной степени.

УТВЕРЖДЕНИЕ: Обозначим идеал $k[t]P(t)$, порожденный полиномом $P(t)$, за (P). Полином $P(t)$ **неприводим тогда и только тогда, когда факторкольцо $k[t]/(P)$ является полем.**

ОПРЕДЕЛЕНИЕ: Пусть $P(t) \in k[t]$ – неприводимый полином. Поле $k[t]/(P)$ называется **расширение k, полученное добавлением корня $P(t)$**. Расширение $[k[t]/(P) : k]$ называется **примитивным**.

УТВЕРЖДЕНИЕ: Пусть $[K : k]$ – конечное расширение. **Тогда K может быть получено из k последовательностью примитивных расширений.** Иначе говоря, существует набор промежуточных расширений $[K = K_n : K_{n-1} : K_{n-2} : ... : K_0 = k]$, таких, что каждое $[K_i : K_{i-1}]$ примитивно.

Расширения Галуа (повторение)

ОПРЕДЕЛЕНИЕ: Пусть $[K : k]$ – конечное расширение поля k. Говорят, что $[K : k]$ **расширение Галуа**, если $K \otimes_k K$ изоморфно (как кольцо) прямой сумме нескольких копий K.

ТЕОРЕМА: Пусть $K \supset K' \supset k$ – цепочка конечных расширений. Предположим, что $[K : k]$ – расширение Галуа. **Тогда $[K : K']$ тоже расширение Галуа.**

ТЕОРЕМА: Пусть $P(t) \in k[t]$ – неприводимый полином степени n, имеющий n попарно различных корней $\alpha_1, ..., \alpha_n$ в конечном расширении $[K : k]$. Предположим, что K порождено $\{\alpha_i\}$. **Тогда это расширение Галуа.**

ОПРЕДЕЛЕНИЕ: Пусть $[\overline{k} : k]$ – алгебраическое замыкание k, а $K \subset \overline{k}$ – поле, полученное из k добавлением всех корней $\alpha_i \in \overline{k}$. Тогда K называется **полем разложения $P(t)$.**

ЗАМЕЧАНИЕ: В характеристике 0, поля разложения суть поля Галуа (в характеристике p, не обязательно)

УТВЕРЖДЕНИЕ: Если $[K : k]$ – конечное расширение, $\operatorname{char} k = 0$, то **существует расширение $[K_1 : K]$ такое, что $[K_1 : k]$ – расширение Галуа.**

Группа Галуа (повторение)

ОПРЕДЕЛЕНИЕ: Пусть $[K : k]$ – расширение Галуа. **Группой Галуа** $[K : k]$ называется группа $\mathrm{Aut}_k(K)$ k-линейных автоморфизмов поля K.

УТВЕРЖДЕНИЕ: Пусть $[K : k]$ – расширение Галуа. Тогда **существует естественная биекция между следующими множествами.**

(а) Группой Галуа $\mathrm{Aut}_k(K)$

(б) Простые идеалы в $K \otimes_k K$.

СЛЕДСТВИЕ: Порядок группы Галуа равен степени $[K : k]$**.**

СЛЕДСТВИЕ: Пусть $[K : k]$ – расширение Галуа. Рассмотрим действие группы Галуа $\mathrm{Aut}_k(K)$ на $K \otimes_k K$ автоморфизмами, $\zeta(a \otimes b) = a \otimes \zeta(b)$. **Это действие транзитивно на компонентах разложения в прямую сумму** $K \otimes_k K = \bigoplus K$**.**

СЛЕДСТВИЕ: Пусть $[K : k]$ – расширение Галуа, которое примитивно: $K = k[t]/(P)$, где $P(t) \in k[t]$. **Тогда** $\mathrm{Aut}_k(K)$ **действует транзитивно на корнях** $P(t)$**.**

Основная теорема теории Галуа (повторение)

ЛЕММА: Пусть $[K:k]$ – расширение Галуа, а $G' \subsetneq \mathrm{Aut}_k K$ есть нетривиальная подгруппа группы Галуа. **Тогда** $K^{G'} \neq k$.

ЛЕММА: Пусть $[K:k]$ – расширение Галуа, а $a \in K$ – элемент, инвариантный относительно $\mathrm{Aut}_k(K)$. **Тогда** $a \in k \subset K$.

ТЕОРЕМА: (Основная теорема теории Галуа)
Пусть $[K:k]$ – расширение Галуа. Тогда соответствия **стрелки** $G' \longrightarrow K^{G'}$ **и** $K' \longrightarrow \mathrm{Aut}_{K'} K \subset G$ **устанавливают биекцию между множеством подгрупп** $G' \subset \mathrm{Aut}_k(K)$ **и множеством промежуточных подполей** $K \supset K' \supset k$.

Примитивные расширения

ОПРЕДЕЛЕНИЕ: Расширение $[K:k]$ называется **сепарабельным**, если форма следа на K невырождена.

УПРАЖНЕНИЕ: Докажите, что следующие условия равносильны.

(i) $[K:k]$ сепарабельно

(ii) $K \otimes_k K$ не содержит нильпотентов.

(iii) Для любого $x \in K$, минимальный многочлен $P_x(t) \in k[t]$ не имеет кратных корней.

ТЕОРЕМА: (теорема Артина о примитивном элементе)
Пусть $[K:k]$ – конечное расширение, причем K бесконечно, и выполнено одно из условий: (1) $\operatorname{char} k = 0$ (2) $[K:k]$ – подполе в расширении Галуа (3) $[K:k]$ сепарабельно. **Тогда $[K:k]$ примитивно**, то есть порождено одним элементом $x \in K$.

ЗАМЕЧАНИЕ: Первые два утверждения были доказаны на прошлой лекции, 3-е оставлено в качестве упражнения.

Циклотомические расширения

ОПРЕДЕЛЕНИЕ: **Циклотомическое расширение** есть поле разложения для многочлена $P(t) := \sum_{i=0}^{n-1} t^i$.

ЗАМЕЧАНИЕ: $P(t) = \frac{t^n-1}{t-1}$, то есть **циклотомическое расширение получается добавлением всех корней степени n из единицы.**

УТВЕРЖДЕНИЕ: **Группа корней степени n из единицы циклическая.**

ДОКАЗАТЕЛЬСТВО: Дословно то же самое, что для $\mathbb{F}_{p^n}$. ■

ОПРЕДЕЛЕНИЕ: $\varepsilon \in \mathbb{C}$ называется **примитивным корнем**, или же **первообразным корнем** степени n из единицы, если ε порождает группу корней степени n.

Группа Галуа циклотомического расширения

УТВЕРЖДЕНИЕ: Группа Галуа циклотомического расширения вложена в мультипликативную группу $(\mathbb{Z}/n)^*$ остатков, взаимно простых с n.

Доказательство. Шаг 1: Пусть ε есть примитивный корень, а $\nu \in \mathrm{Aut}[K:\mathbb{Q}]$ – элемент группы Галуа. Тогда ν переводит ε в какой-то другой примитивный корень, то есть в ε^a для a, взаимно простого с n. Значит, **группа Галуа циклотомическоро расширения вложена в** $(\mathbb{Z}/n)^*$**, и она действует на корнях, переводя корень** e **в** e^a**.** ■

ЗАМЕЧАНИЕ: На самом деле группа Галуа $\mathrm{Aut}[K:\mathbb{Q}]$ изоморфна группе $(\mathbb{Z}/n)^*$, но доказать это довольно трудно.

Циклические расширения

ОПРЕДЕЛЕНИЕ: Расширение Галуа $[K:k]$ называется **циклическим**, если его группа Галуа циклическая.

УТВЕРЖДЕНИЕ: Пусть поле k содержит все корни степени n из единицы, а $[K:k]$ – поле разложения многочлена $P(t)=t^n-a$, где $a\neq b^l$ для любого $l|n$. Предположим, что $\operatorname{char} p$ не делит n. **Тогда это расширение циклическое.**

Доказательство. Шаг 1: Это расширение Галуа, ибо **если** $\operatorname{char} p$ **не делит** n**, то** $P(t)$ **и** $P'(t)$ **взаимно просты,** а значит, у $P(t)$ нет кратных корней.

Шаг 2: Если α есть корень $P(t)$, можно написать $P(t)=\prod(t-\zeta_i\alpha)$, где $\{\zeta_i\}$ – множество всех корней степени n из 1. Значит, K получается из k добавлением α.

Циклические расширения (окончание)

Шаг 3: Если полином $P(t)$ приводим и раскладывается в произведение $P(t) = Q_1(t)Q_2(t)$, мы имеем $Q_i(t) = \prod(t - \zeta_j\alpha)$, где произведение берется по части корней. Значит, свободный член Q_i имеет вид $\alpha^m\zeta$, где $\zeta \in k$ – корень из единицы. Применив алгоритм Евклида к соотношениям $\alpha^m \in k$ и $\alpha^n \in k$, получим соотношение вида $\alpha^l \in k$ для $l|n$. Значит, $P(t)$ неприводим.

Шаг 4: Пусть ζ – какой-то корень степени n из 1. Рассмотрим автоморфизм $K = k[t]/(P)$, переводящий t в ζt. Группа, порожденная такими автоморфизмами, изоморфна $\mathbb{Z}/n$. **Значит, ее порядок равен степени $[K : k]$.** Поэтому это вся группа Галуа. ■

Резольвента Лагранжа

ТЕОРЕМА: (теорема Куммера) Пусть поле k содержит все корни степени n из единицы, а $[K:k]$ – циклическое расширение степени n. **Тогда** $K = k[t]/(P)$**, где** $P(t) = t^n - a$**.**

Доказательство. Шаг 1: Для конечного поля все уже доказано. Будем доказывать для бесконечного.

Шаг 2: Расширение Галуа всегда примитивно. Пусть ν – образующая группы $G := \mathrm{Aut}_k(K)$, $\xi \in k$ – примитивный корень из единицы степени n, а $a \in K$ – примитивный элемент. Напишем **резольвенту Лагранжа** $L = a + \xi^{-1}\nu(a) + \xi^{-2}\nu^2(a) + \dots + \xi^{-n+1}\nu^{n-1}(a)$. Тогда $\nu(L) = \xi L$.

Шаг 3: Пусть $V \subset K$ – k-векторное подпространство, порожденное $a, \nu(a)$, $\nu^2(a), \dots$ Число G-инвариантных подпространств $V \subsetneq K$ конечно. Выбрав a вне этих подпространств, можно считать, что все $a, \nu(a), \nu^2(a), \dots$ линейно независимы над k, **а значит,** $L \neq 0$**.**

Резольвента Лагранжа (окончание)

УТВЕРЖДЕНИЕ: Пусть поле k содержит все корни степени n из единицы, а $[K:k]$ – циклическое расширение степени n. **Тогда $K = k[t]/(P)$, где $P(t) = t^n - a$.**

Шаг 2: Расширение Галуа всегда примитивно. Пусть ν – образующая группы $G := \mathrm{Aut}_k(K)$, $\xi \in k$ – примитивный корень из единицы степени n, а $a \in K$ – примитивный элемент. Напишем **резольвенту Лагранжа** $L = a + \xi^{-1}\nu(a) + \xi^{-2}\nu^2(a) + \dots + \xi^{-n+1}\nu^{n-1}(a)$. Тогда $\nu(L) = \xi L$.

Шаг 3: Пусть $V \subset K$ – k-векторное подпространство, порожденное $a, \nu(a), \nu^2(a), \dots$ Число G-инвариантных подпространств $V \subsetneq K$ конечно. Выбрав a вне этих подпространств, можно считать, что все $a, \nu(a), \nu^2(a), \dots$ линейно независимы над k, **а значит, $L \neq 0$.**

Шаг 4: Тот же аргумент показывает, что **можно выбрать a таким образом, что L тоже примитивно.**

Шаг 5: $\prod_{i=0}^{n-1}(t-\nu^i(L)) = t^n - L^n$, но L^n инвариантно относительно $\mathrm{Aut}_k(K)$, а значит, лежит в k. **Мы получаем, что $K = k[t]/(P)$, где $P(t) = t^n - L^n$.**
■

Расширения Галуа и корни

ТЕОРЕМА: Пусть $[K:k]$ – конечное, сепарабельное, примитивное расширение. Тогда следующие условия равносильны.

(i) $[K:k]$ **– расширение Галуа.**

(ii) **Для любого** $x \in K$**, все корни его минимального многочлена** $P_x(t) \in k[t]$ **содержатся в** K.

Доказательство. Шаг 1: Импликация (ii) $\Rightarrow$ **(i) следует из теоремы о примитивном элементе,** ибо $K = k[x]$ есть поле разложения многочлена $P_x(t) \in k[t]$.

Шаг 2: Пусть K – расширение Галуа, $x \in K$, а $K' := k[x]$ – порожденное им подполе. Тогда $K' \otimes_k K$ есть подкольцо в $K \otimes_k K = \bigoplus K$. Поскольку $K' \otimes_k K$ линейно относительно умножения на K справа, $K' \otimes_k K$ **– тоже прямая сумма нескольких копий** K**.**

Шаг 3: Поскольку $K' = k[t]/(P_x)$, $K' \otimes_k K = K[t]/(P_x)$, а **коль скоро все слагаемые** $K[t]/(P_x)$ **одномерны над** K**, многочлен** $P_x(t)$ **разлагается на линейные множители в** $K[t]$**.** Это доказывает импликацию (i) $\Rightarrow$ (ii).
■

Группа Галуа и корни

УТВЕРЖДЕНИЕ: Пусть $[K : k]$ – расширение Галуа, $x \in K$, а $P_x(t) \in k[t]$ его минимальный многочлен. **Тогда группа Галуа** $\mathrm{Aut}_k(K)$ **действует транзитивно на корнях** $P_x(t)$**.**

ДОКАЗАТЕЛЬСТВО: Все коэффициенты многочлена $\prod_{\in\in \mathrm{Aut}_k(K)}(t - \nu(x)$ $\mathrm{Aut}_k(K)$-инвариантны, значит, лежат в k. Поэтому этот многочлен делится на $P_x(t)$. ■

Последовательности расширений Галуа

ТЕОРЕМА: Пусть $[K : K' : k]$ конечные расширения, причем $[K : k]$ – расширение Галуа. Тогда следующие условия равносильны.

(i) $[K' : k]$ **– расширение Галуа.**

(ii) Группа Галуа $\operatorname{Aut}_{K'}(K)$ **– нормальная подгруппа в** $\operatorname{Aut}_k(K)$**.**

(iii) **Действие** $\operatorname{Aut}_k(K)$ **сохраняет** $K' \subset K$**.**

В этой ситуации, $\operatorname{Aut}_k(K') = \operatorname{Aut}_k(K)/\operatorname{Aut}_{K'}(K)$.

Доказательство. Шаг 1: Подполя в $K \supset K'' \supset k$ находятся в биективном соответствии с подгруппами в $\operatorname{Aut}_k(K)$. Группа Галуа $G := \operatorname{Aut}_k(K)$ переставляет подгруппы G, действуя на них сопряжениями. **Нормальные подгруппы суть такие, которые неподвижны при действии** G**.** Поэтому соответствующие поля – тоже неподвижны (при действии G на K). Это доказывает равносильность (ii) и (iii).

Последовательности расширений Галуа (окончание)

ТЕОРЕМА: Пусть $[K : K' : k]$ конечные расширения, причем $[K : k]$ – расширение Галуа. Тогда следующие условия равносильны.

(i) $[K' : k]$ **– расширение Галуа.**

(ii) Группа Галуа $\operatorname{Aut}_{K'}(K)$ **– нормальная подгруппа в** $\operatorname{Aut}_k(K)$**.**

(iii) **Действие** $\operatorname{Aut}_k(K)$ **сохраняет** $K' \subset K$**.**

Шаг 2: Пусть $x \in K'$ – какой-то элемент, а $P_x(t) \in k[t]$ – его минимальный полином. В силу предыдущей теоремы, K' есть расширение Галуа тогда и только тогда, когда $P_x(t)$ разложим в K', причем в этом случае G действует на его корнях транзитивно. **Группа Галуа** G **переставляет корни многочлена** $P_x(t)$**, действуя на них транзитивно.** Значит, если G сохраняет K', все корни $P_x(t)$ лежат в K'. Это доказывает импликацию (iii) $\Rightarrow$ (i).

Шаг 3: Если же $[K' : k]$ – расширение Галуа, то G **сохраняет** K'**, потому что она переставляет корни многочленов** $P(t) \in k[t]$**,** а для каждого корня $P(t)$, содержащегося в K', все остальные тоже там содержатся.

Шаг 4: Изоморфизм $\operatorname{Aut}_k(K') = \operatorname{Aut}_k(K)/\operatorname{Aut}_{K'}(K)$ следует из того, что $\operatorname{Aut}_k(K)$ действует на K' автоморфизмами, без инвариантов, а ядро отображения $\operatorname{Aut}_k(K) \longrightarrow \operatorname{Aut}_k(K')$ есть $\operatorname{Aut}_{K'}(K)$. ■

Разрешимые группы

ОПРЕДЕЛЕНИЕ: Группа G называется **разрешимой**, если содержит цепочку нормальных подгрупп $G = G_0 \supset G_1 \supset ... \supset G_n = \{e\}$, причем каждая из факторгрупп коммутативна.

УТВЕРЖДЕНИЕ: Пусть расширение Галуа $[K : k]$ содержит цепочку подполей $K = K_1 \supset K_2 \supset ... \supset K_n = k$ со следующими свойствами:

(i) Для всех i, $[K_i : k]$ – расширение Галуа.

(ii) Группа Галуа $\mathrm{Aut}_{K_{i+1}}(K_i)$ абелева.

Тогда группа Галуа $[K : k]$ разрешима. Обратное тоже верно: **каждое расширение с разрешимой группой Галуа может быть получено таким образом.**

ДОКАЗАТЕЛЬСТВО: Сразу следует из предыдущей теоремы. ■

Теорема Абеля

ТЕОРЕМА: (теорема Абеля)
Пусть поле k содержит все корни из 1, а расширение Галуа $[K : k]$ содержит цепочку подполей $K = K_1 \supset K_2 \supset ... \supset K_n = k$ со следующими свойствами:

(i) Для всех i, $[K_i : k]$ – расширение Галуа.

(ii) Расширение $[K_i : K_{i-1}]$ получено добавлением корней многочлена $P(t) = t^{n_i} - a_i$.

Тогда группа Галуа $\mathrm{Aut}_k(K)$ **разрешима.** Обратное тоже верно: **любое расширение Галуа** $[K : k]$ **с разрешимой группой Галуа может быть получено таким образом.**

ДОКАЗАТЕЛЬСТВО: Разрешимость $\mathrm{Aut}_k(K)$ следует из предыдущего утверждения, и вычисления группы Галуа для циклического расширения. Обратное утверждение следует из теоремы Куммера, утверждающей, что каждое циклическое расширение получено добавлением корней многочлена $P(t) = t^{n_i} - a_i$. ■

СЛЕДСТВИЕ: (теорема Абеля)
Полиномиальное уравнение разрешимо в радикалах тогда и только тогда, когда его группа Галуа разрешима.

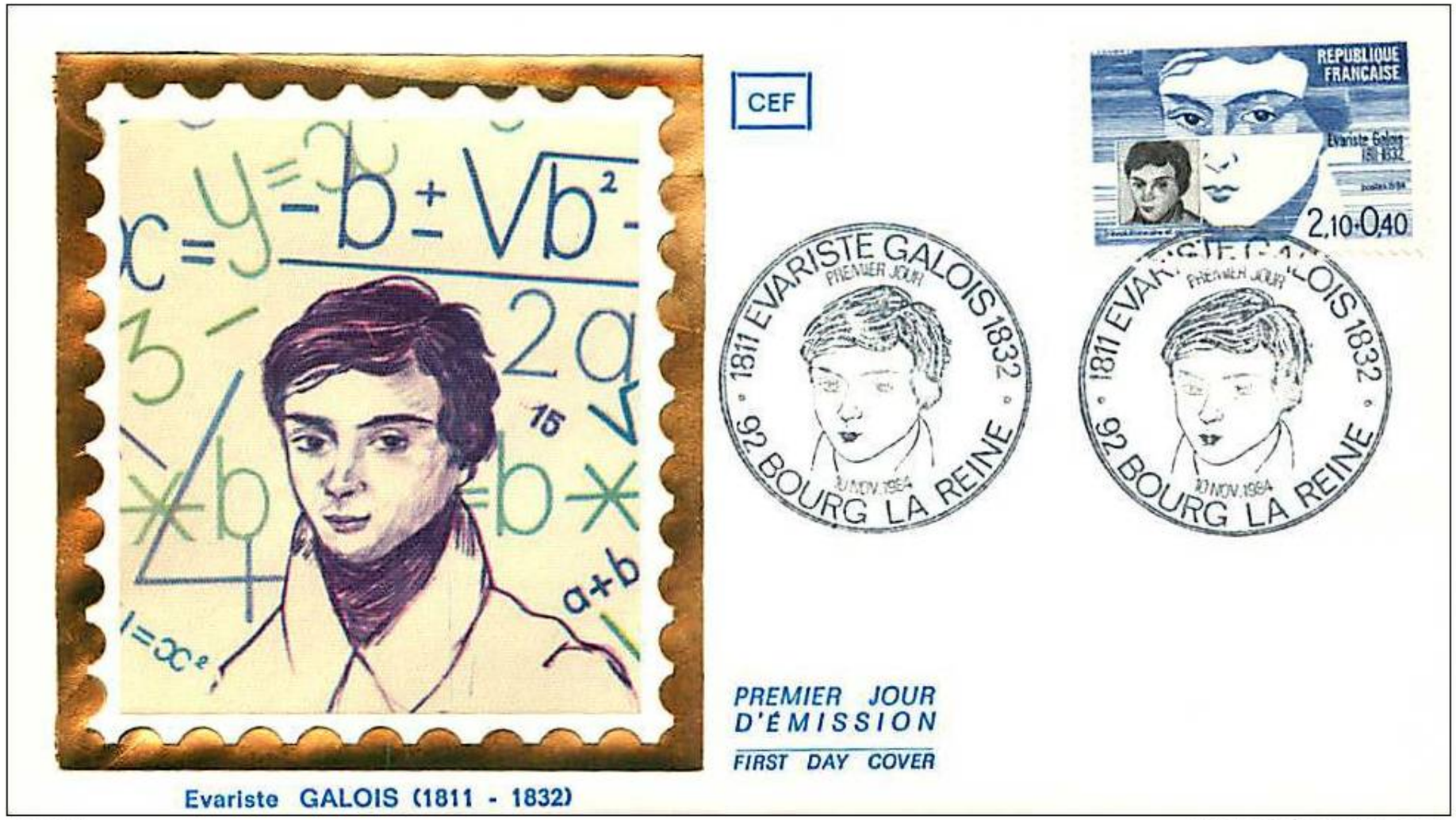
Экзамены, сессия

В следующую пятницу (22.03.2013), будет коллоквиум в виде устной контрольной. Письменная контрольная (тоже задачи) будет 29.03.2013, с 12:00 до 15:30.

Вместе с решениями, 29 марта студенты **должны сдать копии своих ведомостей,** с отметками о том, **сколько баллов им причитается за каждый листочек**, и кратким объяснением, почему именно столько. Показ работ и окончательная расстановка оценок – среда, 3-го апреля (первая половина дня).

Студенты, которые не сдадут свои ведомости 29-го, ничего за листочки не получат (или получат, но не сразу и без удовольствия).

Окончательная оценка вычисляется по формуле $F = 0.1B$, где B есть сумма баллов за все (округление вниз).


CEF
1811 EVARISTE GALOIS 1832
PREMIER JOUR
92 BOURG LA REINE
30 NOV. 1984
REPUBLIQUE FRANCAISE
Evariste Galois
1811-1832
2,10+0,40
PREMIER JOUR
D'ÉMISSION
FIRST DAY COVER
Evariste GALOIS (1811 - 1832)
Memphre
www.delcampe.net