Что такое закон взаимности? 5/8/2011

К. Конрад Задание 4

1. Пусть F – поле характеристики 2. Для элементов a и b в $F^\times$, определяем алгебру кватернионов

$$[a,b)_F = F + Fi + Fj + Fk,$$

где $i^2 + i = a$ (вместо $i^2 = a$!), $j^2 = b$, и $k = ij = j(i+1)$.

   (a) Выведите прямо из определения, что центр этой алгебры – F.

   (b) Для $q = x+yi+zj+tk \in [a,b)_F$, где $x, y, z, t \in F$, пусть $\overline{q} = x+y(i+1)+zj+tk$ и $\mathrm{N}(q) = q\overline{q}$. Найдите формулу для $\mathrm{N}(q)$ в терминах координат q и проверьте то, что $\mathrm{N}(q) = \overline{q}q$.

   (c) Если многочлен $T^2 + T + a \in F[T]$ – неприводимый, то покажите, что $[a,b)_F$ является циклической алгеброй $(E/F, \sigma, c)$ для некоторых E, σ, и $c \in F^\times$.

   (d) Если $T^2 + T + a$ приводим над F, покажите, что алгебра $[a,b)_F$ изоморфна $\mathrm{M}_2(F)$.

   (e) Для $a \in F$ и $b \in F^\times$, пусть $((a,b))_F = F + Fi + Fj + Fk$, где $i^2 = a$, $j^2 = b$, и $k = ij = ji + 1$. Проверьте, что $((a,b))_F \cong [ab,b)_F$, используя другой базис алгебры $((a,b))_F$.

2. Используя то, что группа $(\mathbf{Z}/p\mathbf{Z})^\times$ – циклическая, когда p простое, покажите двумя методами, что для всех *нечетных* простых p и целых $k \geq 1$, группа $(\mathbf{Z}/p^k\mathbf{Z})^\times$ – циклическая.

   (a) Порядок группы $(\mathbf{Z}/p^k\mathbf{Z})^\times$ равен $p^{k-1}(p-1)$. Если мы имеем элементы a и b порядка p^{k-1} и $p-1$ соответственно, то ab имеет порядок $p^{k-1}(p-1)$. Покажите, что $1 + p \bmod p^k$ имеет порядок p^{k-1} и используйте лемму Гензеля чтобы показать, что уравнение $x^{p-1} - 1$ имеет $p-1$ решения в $(\mathbf{Z}/p^k\mathbf{Z})^\times$, одно из которых имеет порядок $p-1$.

   (b) Пусть g – целое такое, что $g \bmod p$ порождает группу $(\mathbf{Z}/p\mathbf{Z})^\times$. Покажите, что целое g или $g+p$ порождает группу $(\mathbf{Z}/p^2\mathbf{Z})^\times$ и всякое

целое, которое порождает группу $(\mathbf{Z}/p^2\mathbf{Z})^\times$ также порождает группу $(\mathbf{Z}/p^k\mathbf{Z})^\times$ для всех $k \geq 1$.

Заключите, что для всякого нечетного простого p и целого $k \geq 1$, функция $\chi\colon (\mathbf{Z}/p^k\mathbf{Z})^\times \to \{\pm 1\}$, заданая формулой $\chi(a \bmod p^k) = (\frac{a}{p})$ – единственный нетривиальный гомоморфизм из $(\mathbf{Z}/p^k\mathbf{Z})^\times$ в $\{\pm 1\}$.

3. Для каждого простого $p \equiv 3 \bmod 4$, выведите из определения, что элемент Фробениуса $\mathrm{Frob}_p(\mathbf{Q}(i)/\mathbf{Q})$ является комплексным сопряжением.

4. Пусть $K = \mathbf{Q}(i, \sqrt[4]{3})$. Тогда $\mathrm{Gal}(K/\mathbf{Q}) = \{1, r, r^2, r^3, s, rs, r^2s, r^3s\}$, где

$$r(i) = i, r(\sqrt[4]{3}) = i\sqrt[4]{3}, \quad s(i) = -i, s(\sqrt[4]{3}) = \sqrt[4]{3}.$$

   (a) Проверьте, что классы сопряженности в группе Галуа следующие:

$$\{1\}, \quad \{r, r^3\}, \quad \{r^2\}, \quad \{s, r^2s\}, \quad \{rs, r^3s\}.$$

   (b) Проверьте, что элемент Фробениуса на простом числе 5 удовлетворяет условию $\sigma(i) = i$, поэтому $\sigma \in \{1, r, r^2, r^3\}$. Объясните почему класс сопряженности Фробениуса простого 3 есть $\{r, r^3\}$.

   (c) Покажите, что классом сопряженности Фробениуса простого числа 7 является $\{rs, r^3s\}$.

5. В лекции было сказано, что из закона взаимности Артина над $\mathbf{Q}$ следует, что всякий гомоморфизм $\rho\colon \mathrm{Gal}(K/\mathbf{Q}) \to \mathbf{C}^\times$ из абелевой группы Галуа над $\mathbf{Q}$ связан с харакетером Дирихле. Если, обратно, мы имеем гомоморфизм $\rho\colon \mathrm{Gal}(K/\mathbf{Q}) \to \mathbf{C}^\times$, где $\mathrm{Gal}(K/\mathbf{Q})$ – абелева и мы знаем, что существует характер Дирихле $\chi\colon (\mathbf{Z}/M\mathbf{Z})^\times \to \mathbf{C}^\times$ по некоторому модулю M т.ч. $\chi(p \bmod M) = \rho(\mathrm{Frob}_p(K/\mathbf{Q}))$, следует ли отсюда закон взаимности Артина над $\mathbf{Q}$ в той форме, как он был сформулирован в лекции?

6. Если положить $p^* = (-1)^{(p-1)/2}p$ для нечетного простого p, мы имеем $p^* \equiv 1 \bmod 4$, поэтому расширение $\mathbf{Q}(\sqrt{p^*})/\mathbf{Q}$ разветвлено только в простом p (в частности, не в 2). Когда π – примарное простое число в $\mathbf{Z}[i]$, квадратичное расширение $\mathbf{Q}(i, \sqrt{\pi})/\mathbf{Q}$ разветвлено только в простом π (например, не в простом $1 + i$)?