PROBLEM SET 10 – DUE THURSDAY AUGUST 12.

Commutators and nontrivial characters

In the first half of the class, the key property of A_5 that we used was that it had no nontrivial characters. In the second half, the key property was that it was its own commutator subgroup (see Problem Set 9). In this section, we will relate these two ideas.

Problem 1. Let A be a finite abelian group with more than one element. In this problem, we will show that A has a nontrivial character. Our proof is by induction on $|A|$. Let g be an element of A, other than e. Let $\langle g \rangle$ be the subgroup $\{g^k : k \in \mathbb{Z}\}$ of A.

(1) Suppose that $\langle g \rangle = A$. Show that A has a nontrivial character.
(2) Suppose that $\langle g \rangle \neq A$. By induction, $A/\langle g \rangle$ has a nontrivial character. Show that A also has a nontrivial character.

Problem 2. Let G be a finite group and let G' be its commutator subgroup.

(1) Suppose that $G' = G$. Show that G has no nontrivial characters.
(2) Suppose that $G' \neq G$. Show that χ has a nontrivial character.

Algebraic integers

Problem 3. We start with a variant of the Key Lemma of Linear Algebra for $\mathbb{Z}$:

(1) Let A_1, A_2, A_3, ... be an infinite sequence of integers. Show that there is some positive integer N and some integers x_1, x_2, ..., x_{N-1} such that $A_N = x_1 A_1 + \cdots + x_{N-1} A_{N-1}$.
(2) Let A_{ij} be an $m \times \infty$ matrix of integers. Show that there is some positive integer N and some integers x_1, x_2, ..., x_{N-1} such that $\sum_{j=1}^{N-1} A_{ij} x_j + A_{iN} = 0$ for $1 \leq i \leq m$.

A complex number α is called an ***algebraic integer*** if there is an **monic** polynomial $f(x) = x^M + f_{M-1} x^{M-1} + \cdots + f_1 x + f_0$ with coefficients in $\mathbb{Z}$ such that $f(\alpha) = 0$.

Problem 4. (1) Let α be an algebraic integer and let $f(x) = x^M + f_{M-1} x^{M-1} + \cdots + f_1 x + f_0$ be a monic polynomial with coefficients in $\mathbb{Z}$ such that $f(\alpha) = 0$. Show that every element of $\mathbb{Z}[\alpha]$ can be written as $\sum_{i=0}^{M-1} a_i \alpha^i$ for integers a_0, a_1, ..., a_{M-1}.
(2) Let α and β be algebraic integers. Let $f(x) = x^M + \cdots + f_0$ and $g(x) = x^N + \cdots + g_0$ be monic integer polynomials with $f(\alpha) = g(\beta) = 0$. Show that every element of $\mathbb{Z}[\alpha, \beta]$ can be written as $\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} c_{ij} \alpha^i \beta^j$ for some MN integers c_{ij}.
(3) Show that every element of $\mathbb{Z}[\alpha, \beta]$ is an algebraic integer.

The factorization of $x^q - x$ modulo p

On the number theory problem sets, many of you discovered the identity

$$x^{p^n} - x = \prod_{f(x) \text{ irreducible, } \deg f | n} f(x)$$

in $\mathbb{F}_p[x]$. We have the tools necessary to prove it.

Problem 5. Let $f(x)$ be an irreducible polynomial in $\mathbb{F}_p[x]$, let d be the degree of $f(x)$ and let $q = p^n$. Set $F = \mathbb{F}_p[t]_{f(t)}$.

(1) Show that $x^q - x$ is not divisible by $f(x)^2$.

So $f(x)$ either divides $x^q - x$ once or no times. We first show that, if $d|n$, then $f(x)|x^q - x$.

(2) Show that the element u of F obeys the equation $u^{p^d} = u$.
(3) Show that $f(x)$ divides $x^{p^d} - x$ in $\mathbb{F}_p[x]$.
(4) Suppose that $d|n$. Show that $f(x)$ divides $x^q - x$ in $\mathbb{F}_p[x]$.

We now show that, if $f(x)|x^q - x$, then $d|n$. We defined $\mathbb{F}_q$ to be the splitting field of $x^q - x$.

(5) Suppose that $f(x)$ divides $x^q - x$. Show that we can embed F as a subfield of $\mathbb{F}_q$.
(6) Suppose that $f(x)$ divides $x^q - x$. Show that $d|n$. Hint: Here is where you use bases.