MATH 435 ASSIGNMENT 12

ARNOLD JIADONG YU

1. Finite Fields

1.1. 24. Show that any finite subgroup of the multiplicative group of a field is cyclic.
proof: Let F be a field, then there are two cases. Let G be an arbitrary finite subgroup of the multiplicative group of F where $G = \{g_1, ..., g_n\}$ for some integer n.

(1) char$(F) = 0$. i.e. F is an extension of Q, and $|G| = n \implies g_i^n = 1$ for every i. Moreover, g_i are zeros of $x^n - 1$ over Q, then

$$x^n - 1 \text{ splits in } Q(g_1, ..., g_n) \text{ where } Q(g_1, ..., g_n) \text{ is an extension of } Q$$

i.e. $Q(g_1, ..., g_n)$ is a field. G is finite subgroup, then by Fundamental Theorem of Finite Abelian Group

$$G \cong \oplus Z_{p_i^{n_i}}$$

where p_i are primes. Moreover, $\gcd(p_i^{n_i}, p_j^{n_j}) = 1$ for $i \neq j$. Every Z_{p_i} is cyclic group with respect to multiplication. i.e. G is generated by the direct sum of generator in each Z_{p_i}. Hence, G is cyclic.

(2) char$(F) = p$ where p is a prime number. F is an extension of Z_p, and $|G| = n \implies g_i^n = 1$ for every i. Moreover, g_i are zeros of $x^n - 1$ over Z_p, then

$$x^n - 1 \text{ splits in } Z_p(g_1, ..., g_n) \text{ where } Z_p(g_1, ..., g_n) \text{ is a finite extension of } Z_p$$

i.e. $Z_p(g_1, ..., g_n)$ is a finite field. i.e. $Z_p(g_1, ..., g_n) \cong Z_{p_1}$ where p_1 is prime. Since Z_{p_1} is cyclic, i.e. $Z_p(g_1, ..., g_n)$ is also cyclic. It follows that the subgroup of a cyclic group is also cyclic. Hence any finite subgroup of the multiplicative group of a finite field is cyclic.
Hence, statement proved by both part 1 and 2.

1.2. 36.*

1.3. 16. Let R be an integral domain that contains a field F as a subring. If R is finite dimensional when viewed as a vector space over F, prove that R is a field.
proof: WTS every element in R has any inverse. Let n be the dimension of R. Let $r \in R\backslash\{0\}$, $f \in F$, then $fr^m \in R$ for any $m \in N$. Construct an explicit set $\{1, r, ..., r^n\} = R_1 \subset R$, then R_1 is linearly dependent since $|R_1| = n + 1 > n$. Let $a_i \in F$, then

$$a_n r^n + a_{n-1} r^{n-1} + ... + a_1 r + a_0 = 0$$

has an nontrivial solution since R is an integral domain. WLOG, assume $a_0 \neq 0$, then

$$a_n r^n + a_{n-1} r^{n-1} + ... + a_1 r = -a_0 \implies r(a_n r^{n-1} + ... + a_1) = -a_0$$
$$\implies r(-\frac{a_n}{a_0} r^{n-1} - ... - \frac{a_1}{a_0}) = 1$$

since $a_0 \in F$, then $a_0^{-1} \in F$. i.e. $\frac{a_i}{a_0} \in F$ for $1 \leq i \leq n$. Therefore, for any $r \in R\backslash\{0\}$, r^{-1} is in R. Hence, R is a field.