August 2016

miércoles, 12 de julio de 2023 3:58 p.m.

① Let G be a group. Show that if the automorphism group $\mathrm{Aut}(G)$ of G is cyclic, then G is abelian. [Hint: Consider the map $G \to \mathrm{Aut}(G)$ given by $g \mapsto \gamma_g$, where $\gamma_g(x) = gxg^{-1}$ for all $x \in G$. What is the kernel of this map?]

Pf: Let $\gamma: G \to \mathrm{Aut}(G)$ be the homomorphism described in the hint, so γ_g is conjugtion by g.
To see that γ is a homomorphism:
$\gamma_{gh}(x) = ghx(gh)^{-1} = ghxh^{-1}g^{-1} = g\gamma_h(x)g^{-1} = (\gamma_g \circ \gamma_h)(x)$
We see that
$$\begin{aligned}\ker(\gamma) &= \{g \in G : \gamma_g = id.\}\\ &= \{g \in G : gxg^{-1} = x \text{ for all } x \in G\}\\ &= \{g \in G : gx = xg \text{ for all } x \in G\}\end{aligned}$$
So $\ker(\gamma) = Z(G)$, the center of G.
From the gp. isomorphism thms., we have $G/Z(G) \cong \gamma(G) \subseteq \mathrm{Aut}(G)$
Since $\mathrm{Aut}(G)$ is cyclic, so is its subgp $\gamma(G)$, so we conclude that $G/Z(G)$ is cyclic. This implies that G is abelian.

To see why, let $x, y \in G$ and let $g \in G$ s.t. $\bar{g}$ generates $G/Z(G)$.
Then we can write $x = x'g^m$ and $y = y'g^n$ where $x', y' \in Z(G)$.
Then
$$\begin{aligned}xy &= x'g^m y'g^n\\ &= y'x'g^m g^n, \quad y' \in Z(G)\\ &= y'g^m g^n x', \quad x' \in Z(G)\\ &= y'g^n g^m x', \quad \text{powers of } G \text{ commute}\\ &= yx.\end{aligned}$$
□

② (a) Let $G = \{x_1, \dots, x_n\}$ be a finite (multiplicative) abelian group of order n. Show that if G has no element of order 2, then $x_1 \cdot x_2 \cdot \dots \cdot x_n = 1$ and if G has a unique element x of order 2, then $x_1 \cdot x_2 \cdot \dots \cdot x_n = x$.

Pf: In either case, note that if an elt. x_i is not self-inverse, then both x_i and its inverse appear in the product $x_1 \cdots x_n$.
For each pair (x_i, x_i^{-1}) of elts. that are not self-inverse, delete both x_i and x_i^{-1} from the product.
This does not change the value of the product b/c the gp. is abelian and $x_i x_i^{-1} = 1$.
The only elts. that remain after this process is applied are those that are self-inverse (i.e., that have order dividing 2).
- If there is no elt. of order 2, then the product has value 1.
- If there is a unique element x of order 2, the product is just x.

□

(b) For each prime number p, use (a) for a well-chosen G (depending on p) to show that $(p-1)! \equiv -1 \bmod p$.

Pf: For each prime p, choose $G = (\mathbb{Z}/(p))^\times$.
In the case $p = 2$, there is really nothing to show, since $(2-1)! \equiv 1! \equiv -1 \bmod 2$.
For $p > 2$, notice that G contains an elt. of order 2, namely -1 (which is diff. than 1 b/c $p > 2$).
Because $\mathbb{Z}/(p)$ is a field, the equation $x^2 = 1$ has at most two solns, and we see that both 1 and -1 are these solns.
Since 1 has order 1, we conclude that G has a unique element of order 2.
Applying part (a), we see $1 \cdot 2 \cdot \dots \cdot (p-1) \equiv (p-1)! \equiv -1 \bmod p$.
□

③ (a) Show every group of order $7^2 \cdot 11^2$ is abelian.

Pf: Let G be any gp. of order $7^2 \cdot 11^2$.
By the first Sylow thm., we know there exists a 7-Sylow subgp. denoted P s.t. $|P| = 7^2 = 49$, and an 11-Sylow subgp. denoted Q s.t. $|Q| = 11^2 = 121$.
By the third Sylow thm.,
$n_7 \mid 11^2 = 121$ and $n_7 \equiv 1 \bmod 7 \Rightarrow n_7 = 1$
$n_{11} \mid 7^2 = 49$ and $n_{11} \equiv 1 \bmod 11 \Rightarrow n_{11} = 1$
Therefore, P is the unique 7-Sylow subgp. of G. $\Rightarrow P \trianglelefteq G$
Q is the unique 11-Sylow subgp. of G. $\Rightarrow Q \trianglelefteq G$
Notice that $P \cap Q$ must be trivial, since by Lagrange's theorem, its order is a common factor of $|P|$ and $|Q|$, which are coprime $(7^2, 11^2) = 1$.
Since P, Q are normal in G, we know PQ is a subgp. of G, and its order is given by $|PQ| = \dfrac{|P||Q|}{|P \cap Q|} = 7^2 \cdot 11^2$.
Since $|PQ| = |G|$, we conclude that $PQ = G$.
The direct product recognition thm. tells us that $G \cong P \times Q$ since P and Q are normal in G with $P \cap Q$ trivial, and $PQ = G$.
Thus G is the direct product of P and Q, so it suffices to show that P and Q are both abelian.
Groups of order p^2 are abelian, where p is any prime.
$$\left.\begin{aligned}|P| = 7^2 &\Rightarrow P \text{ is abelian.}\\ |Q| = 11^2 &\Rightarrow Q \text{ is abelian}\end{aligned}\right\} \Rightarrow G \text{ is abelian.}$$
Thus, every gp. of order $7^2 \cdot 11^2$ is abelian. □

(b) Use (a) to classify all groups of order $7^2 \cdot 11^2$ up to isomorphism.

Pf: By the Fundamental thm. of finite abelian gps., we can write any group G of order $7^2 \cdot 11^2$ (which by part (a) must be abelian) as the direct product of cyclic groups: $G \cong \mathbb{Z}/(n_1) \times \mathbb{Z}/(n_2) \times \dots \times \mathbb{Z}/(n_k)$, where each $n_i \geq 2$ is an integer and
(1) $n_{i+1} \mid n_i$ for $i = 1, \dots, k-1$ and
(2) $n_1 \cdot n_2 \cdot \dots \cdot n_k = 7^2 \cdot 11^2$.
The n_i are called the invariant factors of G.
In the above notation, n_1 must be divisible by each distinct factor of $|G|$, so $77 \mid n_1$.
If $n_1 = 7^2 \cdot 11^2$, we obtain the gp. $\mathbb{Z}/(7^2 \cdot 11^2)$
If $n_1 = 7 \cdot 11^2$, then $n_2 = 7$ and we get $\mathbb{Z}/(7 \cdot 11^2) \times \mathbb{Z}/(7)$.
If $n_1 = 7^2 \cdot 11$, then $n_2 = 11$ and we get $\mathbb{Z}/(7^2 \cdot 11) \times \mathbb{Z}/(11)$.
If $n_1 = 77$, then $n_2 = 77$ and we get $\mathbb{Z}/(77) \times \mathbb{Z}/(77)$.
Since $77 \mid n_1$, we have listed all possibilities. □

④ Let K be a field and let R be the subring of the polynomial ring $K[x]$ given by all polynomials with x-coefficient equal to 0. That is, $R = \{a_0 + a_1x + a_2x^2 + \dots + a_nx^n \in K[x] : a_1 = 0\}$.

(a) Prove x^2 and x^3 are irreducible, but not prime in R. You may use that $K[x]$ is a UFD.

Pf: Since K is a field, we have that $\deg(fg) = \deg(f) + \deg(g)$ whenever f, g are nonzero polynomials in $K[x]$.
The same identity holds for nonzero $f, g \in R$.
- To see that x^2 is irred., notice that $x^2 = fg$ implies that $\deg(f) + \deg(g) = 2$. Since R contains no polynomials of deg. 1, we conclude that one of f, g has deg. 0 and the other has deg. 2.
WLOG, assume $\deg(f) = 0$, i.e., $f \in K^\times$.
But then f is a unit of R (R contains K as a subring).
Hence any factorization of $x^2 = fg$ must be a product of a unit and an associate of x^2. $\Rightarrow x^2$ is irred. in R.
- A similar argument shows x^3 is irred.. Let $x^3 = fg$, then WLOG $\deg(f) = 0$ and $\deg(g) = 3$ b/c no poly. has deg 1. So f is a unit. x^3 is irred.
- To see that x^2 is not prime, notice that x^2 divides x^6 because $x^6 = x^4 \cdot x^2$.
However, we can write $x^6 = x^3 \cdot x^3$, and $x^2 \nmid x^3$ in R b/c x^3/x^2 must have deg 1 and R has no elts. of deg. 1.
- Similarly, $x^3 \mid x^6$ b/c $x^6 = x^3 \cdot x^3$, but $x^6 = x^2 \cdot x^4$ and $x^3 \nmid x^2$ b/c $\deg(x^3) = 3 > \deg(x^2) = 2$ and $x^3 \nmid x^4$ b/c x^4/x^3 has deg $1 \notin R$.
- We've used the fact that the of $K[x]$ are exactly the nonzero elements of K. Since R contains all the units of $K[x]$, the units of R are exactly the units of $K[x]$.

□

(b) Use (a) to show that the ideal I of R consisting of all polynomials in R with constant term 0 is not principal.

Pf: I must contain both x^2 and x^3.
If I is to be principal, any generator must be a common factor of x^2 and x^3. But each is irred., and they are not associate (b/c they have diff. degrees).
Hence, their only common factors are units. But I contains no units, b/c each unit in R has nonzero constant term.
□

⑤ Let A be a nonzero ring such that $a^2 = a$ for all $a \in A$. (Examples include $\mathbb{Z}/2\mathbb{Z} \times \dots \times \mathbb{Z}/2\mathbb{Z}$, but these are not the only ones.)

(a) Show A has characteristic 2.

Pf: Write 2 for $1+1$. Then $2^2 = 2$ by the defining property of A.
But we also have $2^2 = (1+1)(1+1) = (1+1) + (1+1) = 2 + 2$ by using the distributive law.
Hence, $2 + 2 = 2$, so that $1 + 1 = 2 = 0$.
Hence, $\mathrm{char}(A) = 2$.
□

(b) If A is finite, show its size is a power of 2.

Pf: For the purposes of this part, forget the multiplicative structure of A, and consider A as only an abelian additive group.
By Cauchy's theorem, if $|A|$ is divisible by a prime p, then A contains an elt. of order p. But every elt. of A has order dividing 2, since $a + a = 0$ (this follows from part (a)).
Hence if $p > 2$, p does not divide $|A|$. Hence the only prime factor of $|A|$ is 2, so $|A|$ is a power of 2.
□

(c) Show every prime ideal in A is maximal.

Pf: First we show that A is commutative.
Let $x, y \in A$. We see
$(x+y)^2 = x^2 + xy + yx + y^2$ and $(x+y)^2 = x + y$, so combining these two eqns., $xy + yx = 0$.
But as in part (a), every elt. of A is its own additive inverse, so $xy = yx$.
Hence A is commutative.
We will use the following two facts about comm. rings R in the rest of the arg.:
- an ideal $I \trianglelefteq R$ is prime iff R/I is a domain.
- an ideal $I \trianglelefteq R$ is maximal iff R/I is a field.

Now let I be a prime ideal of A. Then A/I is an integral domain.
Since $a^2 = a$ for every $a \in A$, we know $a^2 \equiv a \bmod I$.
Since A/I is a domain, we have cancellation, so if $a \not\equiv 0 \bmod I$, we conclude that $a \equiv 1 \bmod I$.
It follows that A/I has two elts., 0 and 1 (we note that $A \neq I$ by defn. of prime ideal, so A/I contains more than 1 elt.).
It is clear that 1 is a unit, so each nonzero elt. of A/I is a unit, i.e., A/I is a field. $\Rightarrow I$ is maximal.
We conclude that I is a maximal ideal.
□

⑥ Give examples as requested, with justification.

(a) An automorphism of S_5 with order 3.

Pf: We know conjugation by a fixed elt. of S_5 is an automorphism.
Let φ denote conj. by (123).
Then φ has order dividing 3, because
$\varphi^3(\sigma) = (123)^3 \sigma (321)^3 = \sigma$ for each $\sigma \in S_5$.
So it suffices to show φ is not the identity.
We see $\varphi(12) = (123)(12)(321) = (32) \neq (12)$.
Thus $|\varphi| = 3$.
□

(b) An irreducible polynomial of degree 10 in $\mathbb{Z}[x]$.

Pf: Take $x^{10} - 2$.
This is Eisenstein at 2, so it is irred. as an elt. of $\mathbb{Q}[x]$.
Now suppose $x^{10} - 2 = g(x)h(x)$ for some $g(x), h(x) \in \mathbb{Z}[x]$, $g(x), h(x)$ both not units of $\mathbb{Z}[x]$.
We know at least one of $g(x), h(x)$ must be a unit in $\mathbb{Q}[x]$ (otherwise we would contradict the irreducibility of $x^{10} - 2$ in $\mathbb{Q}[x]$).
The only units of $\mathbb{Q}[x]$ belong to $\mathbb{Z}[x]$ and are not units of $\mathbb{Z}[x]$ are integers other than ± 1.
But this is a contradiction, b/c the only integer factors of $x^{10} - 2$ in $\mathbb{Z}[x]$ are ± 1.
□

(c) A field of size 4.

Pf: Let $\mathbb{F}_2$ be the integers mod 2.
Then $\mathbb{F}_2[x]$ is a PID, so its maximal ideals are exactly its prime ideals.
In a PID, an elt. is prime iff it's irreducible.
We claim that $x^2 + x + 1$ is irred. in $\mathbb{F}_2[x]$.
Since it is quadratic, it is irred. if it has a root in $\mathbb{F}_2$.
Since $0^2 + 0 + 1 \neq 0$ and $1^2 + 1 + 1 = 1$, we know $x^2 + x + 1$ is irred. and hence prime. Then $K = \mathbb{F}_2[x]/(x^2 + x + 1)$ is a field.
To see that it contains only 4 elts., notice that the relation $x^2 = x + 1$ allows us to write any elt. of K as $a + bx$.
It is clear that $0, 1, x$, and $x + 1$ are distinct elts. of $\mathbb{F}_2[x]/(x^2 + x + 1)$; certainly the diff. of no two of these polynomials is divisible by a quadratic.
□

(d) An infinite field of characteristic 3.

Pf: $\mathbb{F}_3$ has characteristic 3.
Consider the field extn. $\mathbb{F}_3(x)$.
In $\mathbb{F}_3(x)$, we know $n \cdot 1 = 0$ iff $n \cdot 1 = 0$ in $\mathbb{F}_3$ iff $3 \mid n$.
This tells us that $\mathbb{F}_3(x)$ has characteristic 3.
Hence the char. of the rational function field $\mathbb{F}_3(x)$ is 3.
□