# CHM: A.23

Po-Shen Loh

29 March 2001

**Problem 1 (A.23)** *Let $R$ be an infinite ring such that every subring of $R$ different from $\{0\}$ has a finite index in $R$. (By the index of a subring, we mean the index of its additive group in the additive group of $R$.) Prove that the additive group of $R$ is cyclic.*

**Solution:**

Our goal will be to use the Fundamental Theorem of Finitely Generated Abelian Groups, from which we conclude that the additive group of $R$ (let us call it $A$) is isomorphic to $\mathbb{Z}^n$. Then we will use an idea similar to "logarithms" to prove that it is really just $\mathbb{Z}$.

First, we will show that $A$ is torsion free as an abelian group.

**Lemma 1** *$A$ is torsion-free.*

**Proof of Lemma 1:**

We proceed by indirect proof; suppose, for the sake of contradiction, that there exist $n \in \mathbb{Z}$ and $r \in R$ such that $nr = 0$. We can immediately proceed to the case of $n$ prime, because if $n = pq$ for prime $p$, then we can just consider $qr$ instead of $r$. Let $H = \langle r \rangle$ and $K = \langle r^2 \rangle$. By the given information, it is obvious that all subrings of the infinite $R$ must likewise be infinite. We will demonstrate that if $nr$ is indeed zero, then $H$ is finite.

Again we have $|H : K| < \infty$, so let us try to mine something out of the coset structure. Concentrate on the cosets $r + K$, $r^3 + K$, $r^5 + K$, ... (the cosets corresponding to the odd powers of $r$). By finiteness, eventually they will repeat, so we will have the form $r^a - r^b \in K$. Since the elements of $K$ can be written as finite polynomials in $r^2$, by the oddity of $a$ and $b$, we have a nonzero polynomial $f(x) \in \mathbb{Z}[x]$ that evaluates to zero at $r$. But since $n$ is a prime and $nr = 0$, we can work with coefficients in the finite field $\mathbb{Z}_n$; we find a corresponding polynomial $g(x) \in \mathbb{Z}_n[x]$ with the same property. Let $cx^d$ be its leading term. Since $\mathbb{Z}_n$ is a field, we can normalize $g(x)$ by multiplying it by $c^{-1}$. This translates into a relation $x^d = p(x)$ for some integral polynomial $p(x)$ with degree less than $d$. Then all elements of $H$ corresponding to polynomials of degree at least $d$ can be reduced to polynomials of degree under $d$ (replace $x^d$ terms by polynomials of degree less than $d$); so the elements of $H$ can be completely described by the polynomials of finite degree less than $d$ with coefficients in the finite field $\mathbb{Z}_n$;

this is a finite set, so $|H| < \infty$ and we have the contradiction predicted at the beginning. Our lemma is proven.

Next we show that $A$ is finitely generated.

**Lemma 2** *$A$ is finitely generated.*

**Proof of Lemma 2:**

Suppose that there exists a subring $T \subset R$ such that its additive group $B$ is finitely generated by some set $\mathcal{G}$. Now, from the given information, $|A : B| < \infty$, so we have only finitely many cosets. Let $\mathcal{C} = \{c_1, c_2, c_3, \ldots, c_k\}$ be representatives from the cosets, and consider the set $\mathcal{G} \cup \mathcal{C}$. This is a finite set, and it generates $R$, so we only need to find a subring of $R$ with finitely generated additive group. We digress to prove an auxiliary lemma that will provide us with such a subring.

**Sublemma 1** *For any $r \in R$, there exist $n \in \mathbb{Z}$ and $p(x) \in \mathbb{Z}[x]$, with the constant term of $p(x)$ equal to zero, such that $nr = p(r)$. Here, we write $nr$ with $n \in \mathbb{Z}$ and $r \in R$ to denote the summation of $n$ copies of $r$. (If $n$ is negative, we add the appropriate number of copies of $-r$.*

**Proof of Sublemma 1:**

Let subrings $D$ and $E$ be defined as follows: $D = \langle r \rangle$ and $E = 0 \oplus r\mathbb{Z}[r]$. In this definition, $r\mathbb{Z}[r]$ refers to the evaluation at $r$ of all polynomials with zero constant term. Clearly, $E \subset D$, and since $D \subset R$, it follows that $|D : E| < \infty$. Let us look at the cosets $0 + E$, $r + E$, $2r + E$, $3r + E$, ...; since we have a finite index, the cosets must eventuall repeat, so there exist $n \in \mathbb{Z}$ such that $nr \in E$, from which our claim is immediate.

Returning to the problem at hand, let us choose an arbitrary nonzero $r \in R$. Applying the lemma, we find some corresponding polynomial $p(x)$. Let $d$ and $a$ be the respective degree and coefficient of the polynomial's leading term; we will be able to prove that $\langle ar \rangle$ works for $B$. This is because $(ar)^d = a^d r^d = a^{d-1}(ar^d) = a^{d-1}q(r)$ for some $q \in \mathbb{Z}[x]$, and since the degree of $q(x)$ is less than $d$, the final expression can be written as $s(ar)$ for some $s \in \mathbb{Z}[x]$. Since all elements in $\langle ar \rangle$ can be expressed as finite integral polynomials in $ar$, any such polynomial with degree $d$ or higher can be re-expressed as a polynomial of degree less than $d$ by applying the relation $(ar)^d = s(ar)$. Therefore the finite set $\{ar, (ar)^2, (ar)^3, \ldots, (ar)^{n-1}\}$ generates $\langle B \rangle$, as desired. Our lemma is proven.

At this point we can invoke the Fundamental Theorem of Finitely Generated Abelian Groups: $A \cong \mathbb{Z}^n$. The remainder of this proof will show that $n = 1$.

**Lemma 3** $n = 1$.

**Proof of Lemma 3:**

Suppose that the $n$ generators of the free group $A$ are $\{x_1, x_2, \ldots, x_n\}$. Define the family of free subgroups $A_k = \mathbb{Z}x_k$; as we go through the all the powers of $x_i$, we must enter all of the subgroups. That is, for each $A_k$, there exists some

$a_k$ for which $x_i^{a_k} \in A_k$. This is because if we did not enter some subgroup $A_m$, then for every $z \in \mathbb{Z}$ we have a distinct coset $za_m + \langle x_i \rangle$. But $|R : \langle x_i \rangle| < \infty$, so we have a contradiction. Therefore, we must enter every coset as we go through the powers of $x_i$. Let us go through the powers of $x_1$ and see what happens.

Let $\mathcal{S} = \{k \in \mathbb{Z}^+ | x_1^k \in A_1\}$. Clearly, if $a, b \in \mathcal{S}$ then $a + (b-1) \in \mathcal{S}$ because $x_1^{a+b-1} = x_1^{a-1} x_1^b = x_1^a \in A_1$. Similarly, as long as $a-(b-1)$ is positive, it must also be in $\mathcal{S}$. Therefore, since $1 \in \mathcal{S}$, if $2 \in \mathcal{S}$ we will have $\mathcal{S} = \mathbb{Z}^+ \rightarrow n = 1$. This is our final sublemma.

**Sublemma 2** $2 \in \mathcal{S}$.

**Proof of Sublemma 2:**

Again proceed by indirect proof; assume for the sake of contradiction that $2 \notin \mathcal{S}$. Let $y$ be the smallest member of $\mathcal{S}$ other than 1. By the above result, $\mathcal{S}$ must contain all positive integers congruent to 1 modulo $y$, and nothing more. Define $M = \langle x_1 \rangle$ and $N = \langle x_1^y \rangle$. Again $|M : N| < \infty$ so we can extract information by looking at the family of cosets $0+N$, $x_1+N$, $2x_1+N$, $3x_1+N$, ...(this is infinite since $R$ is torsion-free and these are distinct cosets because $\mathcal{S} = \{k \in \mathbb{Z}^+ | k \equiv 1 \pmod{y}\}$). We discover that for some $z \in \mathbb{Z}$, $zx_1 \in N$; the elements of $N$ can be expressed as polynomials in $x_1^y$, so we find $p(x_1) \in A_1$ for some integral polynomial with all exponents divisible by $y$.

Write $p(x_1)$ as $\sum_k c_k x_1^{yk}$. By assumption $y \neq 2$, so none of the terms in $p(x_1)$ are in $A_1$. Therefore when we write $p(x_1) = zx_1$, we have a nontrivial linear dependence relation between the basis elements of our free abelian group. This is a contradiction, so $y = 1$ as required. Our sublemma is proven.

And we are done.