FIELD THEORY HOMEWORK 1 SOLUTIONS

JC

(1) Let $G$ be a group, and recall that if $X \subseteq G$ then $\langle X \rangle$ is the smallest subgroup of $G$ containing $X$. Recall also that $g^h = hgh^{-1}$.

(a) Prove that if $x^h \in X$ for all $x \in X$ and $h \in G$, then $\langle X \rangle \lhd G$.

The elements of $\langle X \rangle$ are finite products of elements of $X$ and their inverses. Since $(xy)^h = x^hy^h$ and $(x^{-1})^h = (x^h)^{-1}$, it is clear that $(X)^h \subseteq \langle X \rangle$ for all $h$, hence it is normal.

(b) Let $G$ be the group whose elements are permutations of $\mathbb{Z}$, with the group operation being composition. Find a subset $X \subseteq G$ such that $X$ is finite, all the elements of $X$ have finite order, and $\langle X \rangle$ is infinite.

Let $\sigma$ be the permutation which exchanges $2n$ and $2n + 1$ for all $n$, while $\tau$ exchanges $2n$ and $2n - 1$ for all $n$. They both have order two, but $\tau\sigma$ moves $2n$ to $2n + 2$ for all $n$ so has infinite order.

(2) Prove that if $R$ is a subring of $S$, and $P$ is a prime ideal of $S$ then $R \cap P$ is a prime ideal of $R$. Does $M$ being maximal in $S$ imply that $R \cap M$ is maximal in $R$?

Proof 1: $1 \notin P$, so that $1 \notin P \cap R$. Also if $r, s \in R$ and $rs \in P \cap R$ then by primeness either $r \in P$ or $s \in P$.

Proof 2: The composition of the inclusion map from $R$ to $S$ and the quotient map from $S$ to $S/P$ has kernel $R \cap P$. Its image is a subring of $S/P$, hence an ID, but also its image is (by the 1st IM theorem) isomorphic to $R/R \cap P$, so $R \cap P$ is prime.

It is false in general that $M$ maximal implies $R \cap M$ maximal. For example $\mathbb{Z}$ is a subring of $\mathbb{Q}$, $(0)$ is maximal in the field $\mathbb{Q}$ but not in the non-field $\mathbb{Z}$.

(3) Let $p$ be a prime number and let $R$ be the subset of $\mathbb{Q}$ consisting of rational numbers of the form $a/b$ where $p$ does not divide $b$. Prove that $R$ is a subring of $\mathbb{Q}$. What are the units of $R$? Prove that $R$ has exactly one maximal ideal.

$R$ is easily seen to be a subring, since $p$ is prime and the sum and product of $a_1/b_1, a_2/b_2$ can both be written with denominator $b_1b_2$.

The units are exactly those rational numbers of form $a/b$ where neither $a, b$ are divisible by $p$. Since a maximal ideal can not contain any units, any maximal ideal is a subset of the non-units. In this ring the non-units are the multiples of $p$, so in fact $(p)$ is the only maximal ideal.

(4) Let $R$ be a ring. Prove that the set of $r \in R$ such that $r^n = 0$ for some $n > 0$ is an ideal of $R$.

0 is clearly such an element. If $r^n = 0$ then $(ar)^n = a^n r^n = 0$. Finally if $r^m = s^n = 0$ then $(r + s)^{m+n}$ can be expanded as a sum of terms $r^is^j$ where $i + j = m + n$, so that either $i \geq m$ or $j \geq n$ and hence $(r + s)^{m+n} = 0$.  

1
Cultural note: this ideal is called the \textit{nilradical} of $R$ and its elements are called \textit{nilpotent}. 