Math 5210 - Abstract Algebra I   Problem Set 5

> *I have often pondered over the roles of knowledge or experience, on the one hand, and imagination or intuition, on the other, in the process of discovery. I believe that there is a certain fundamental conflict between the two, and knowledge, by advocating caution, tends to inhibit the flight of imagination. Therefore, a certain naivete, unburdened by conventional wisdom, can sometimes be a positive asset.* Harish-Chandra

Read: text sections 7.1–7.4, 8.1–8.2

Exercise 1. Let R be a (nonzero) commutative ring. An element $x \in R$ is called *nilpotent* if $x^n = 0$ for some n.

(a) Find all the nilpotent elements of $\mathbb{Z}/(9)$ and $\mathbb{Z}/(27)$.

(b) Describe (with justification) all the nilpotent elements of $\mathbb{Z}/(p^k)$ where p is prime and $k \geq 2$.

(c) Describe (with justification) all the nilpotent elements of $\mathbb{Z}/(20)$ and then all the nilpotent elements of any $\mathbb{Z}/(m)$ for $m \geq 2$. (Note: these are generally *not* all the non-invertible elements!)

(d) Show the nilpotent elements of R form an ideal. (Hint for addition: if $x^n = 0$ and $y^m = 0$, show $(x+y)^{n+m} = 0$ by thinking about what powers of x and y can show up when expanding this power.)

(e) If x is nilpotent, show $1 + x$ is invertible. (Hint: geometric series!)

Solution 1.

Exercise 2. Let K and L be fields and A be a subring of K that admits a homomorphism $f\colon A \to L$. We want to extend f to a homomorphism on larger subrings of K (see diagram below). We can't always extend f all the way to K, *e.g.*, the reduction map $\mathbb{Z} \to \mathbb{Z}/(p)$, for prime p can't be extended to a homomorphism $\mathbb{Q} \to \mathbb{Z}/(p)$.

$$\begin{tikzcd}
K \arrow[d, dash] \\
R \arrow[d, dash] \arrow[dr, dotted, "?"] \\
A \arrow[r, "f"'] & L
\end{tikzcd}$$

(a) If $a \in A - \{0\}$ and $f(a) \neq 0$, show f admits a unique extension to a ring homomorphism $A[1/a] \to L$. (It is insufficient to show there is at most one extension of f to $A[1/a]$: you must show there really is an extension of f to $A[1/a]$.)

(b) Use Zorn's lemma to show there is an extension of f to a ring homomorphism $\widetilde{f}\colon \widetilde{A} \to L$ for some ring $\widetilde{A}$ between A and K, and $\widehat{f}$ can't be extended further to a ring homomorphism $R \to L$ for any R strictly between $\widetilde{A}$ and K.

(c) If $x \in \widetilde{A}$ and $\widetilde{f}(x) \neq 0$, use parts a and b to show $1/x \in \widetilde{A}$. Conclude that $\ker \widetilde{f}$ is a maximal ideal in $\widetilde{A}$, and in fact is the only maximal ideal in $\widetilde{A}$.

Solution 2.

Exercise 3. Let d be a nonsquare integer. For $\alpha = a + b\sqrt{d}$ in $\mathbb{Z}[\sqrt{d}]$, where a and b are integers, we set $\overline{\alpha} = a - b\sqrt{d}$ and $\mathrm{N}(\alpha) = \alpha\overline{\alpha} = a^2 - db^2$. Then $\mathrm{N}(\alpha) \in \mathbb{Z}$, and $\mathrm{N}(\alpha) \neq 0$ if $\alpha \neq 0$. The task of this problem is to give a combinatorial interpretation for $\mathrm{N}(\alpha)$, or rather for $|\mathrm{N}(\alpha)|$.

(a) For nonzero integers m, show $\mathbb{Z}[\sqrt{d}]/(m)$ has size m^2.

(b) For nonzero α, show multiplication by $\overline{\alpha}$ is an additive group isomorphism $\mathbb{Z}[\sqrt{d}]/(\alpha) \to (\overline{\alpha})/(\mathrm{N}(\alpha))$ and conjugation induces an additive group isomorphism $(\alpha)/(\mathrm{N}(\alpha)) \to (\overline{\alpha})/(\mathrm{N}(\alpha))$.

(c) Conclude from parts a and b that the ring $\mathbb{Z}[\sqrt{d}]/(\alpha)$ has size $|\mathrm{N}(\alpha)|$. (Hint: Think of $\mathbb{Z}[\sqrt{d}]/(\alpha)$ as an additive group.)

Solution 3.

Exercise 4. (a) Mimic the proof that $\mathbb{Z}[i]$ is Euclidean to show $\mathbb{Z}[\sqrt{-2}]$ is Euclidean with respect to the function $\mathrm{N}(a + b\sqrt{-2}) = a^2 + 2b^2$. That is, for any α and β in $\mathbb{Z}[\sqrt{-2}]$ with $\beta \neq 0$ show there are γ and ρ in $\mathbb{Z}[\sqrt{-2}]$ such that $\alpha = \beta\gamma + \rho$ and $\mathrm{N}(\rho) < \mathrm{N}(\beta)$.

(b) Mimic the proof that $\mathbb{Z}[i]$ is Euclidean to show $\mathbb{Z}[\sqrt{2}]$ is Euclidean with respect to the function $|\mathrm{N}(a + b\sqrt{2})| = |a^2 - 2b^2|$. That is, for any α and β in $\mathbb{Z}[\sqrt{2}]$ with $\beta \neq 0$ show there are γ and ρ in $\mathbb{Z}[\sqrt{2}]$ such that $\alpha = \beta\gamma + \rho$ and $|\mathrm{N}(\rho)| < |\mathrm{N}(\beta)|$. (Warning: don't make mistakes with inequalities, like saying $|x - y| \leq |x| - |y|$!)

(c) Use your method of proof in parts and b to solve $8 + 20\sqrt{-2} = (5 + 4\sqrt{-2})\gamma + \rho$ in $\mathbb{Z}[\sqrt{-2}]$ with $\mathrm{N}(\rho) < \mathrm{N}(\beta)$ and $27 + 7\sqrt{2} = (7 + 3\sqrt{2})\gamma + \rho$ in $\mathbb{Z}[\sqrt{2}]$ with $|\mathrm{N}(\rho)| < |\mathrm{N}(\beta)|$.

Solution 4.

Exercise 5. Decide which of the following ideals in $\mathbb{Z}[X]$ are prime or maximal by identifying the quotient rings by these ideals with more familiar rings:

(a) (3)

(b) (10)

(c) $(5, X)$

(d) $(X^2 - 3)$

(e) $\{f(X) \in \mathbb{Z}[X] : f(2) = 0\}$.

Solution 5.