METU, Spring 2017, Math 366.

Exercise Set 8

1. Show that every Euclidean domain is a principal ideal domain. Show that every principal ideal domain is a unique factorization domain. Give an example of a unique factorization domain which is not a principal ideal domain. Give an example of a principal ideal domain which is not a Euclidean domain.

2. For each of the following ideals, determine if it is principal or not. If it is principal, find a generator: the ideal $(366, 2013)$ in $\mathbb{Z}$, the ideal $(9+7i, 4+7i)$ in $\mathbb{Z}[i]$, the ideal $(2, 1+\sqrt{-5})$ in $\mathbb{Z}[\sqrt{-5}\,]$, the ideal $(2, x)$ in $\mathbb{Z}[x]$.

3. Let d be a squarefree negative integer. Show that the group of units U of the ring of integers I_d is as follows:
   - For $d=-1$, $U=\{\pm 1, \pm i\}$ where $i=\sqrt{-1}$,
   - For $d=-3$, $U=\{\pm 1, \pm\omega, \pm\omega^2\}$ where $\omega=(\sqrt{-3}+1)/2$,
   - For all other $d<0$, $U=\{\pm 1\}$.

4. Let R be an integral domain and x, y are non-zero elements of R. Show that the following are equivalent:
   (a) x and y are associates, (y is an associate of x if $y=ux$ for some unit u in R.)
   (b) $x|y$ and $y|x$, ($x|y$ if there exists $z \in R$ such that $y=xz$.)
   (c) $(x)=(y)$.

5. Show that $\sqrt{-5}$ is a prime element in I_{-5}. Is $1+\sqrt{-5}$ a prime element? What about $3+2\sqrt{-5}$? Show that 6 and $2\cdot(1+\sqrt{-5})$ do not have a greatest common factor in I_{-5}. Do they have a least common multiple?

6. Show that I_d is not a UFD for $-d \in \{5, 6, 10, 13, 14, 15, 17, 21, 22, 23, 26, 29, 30\}$.

7. Is $10=(3+i)(3-i)=2\cdot 5$ an example of non-unique factorization in $\mathbf{Z}[i]$.

8. If R is a Euclidean domain then show that $(\alpha, \beta)=(\gcd(\alpha, \beta))$ for each pair of nonzero elements α and β.
   (a) Find a generator for the ideal (x^4-1, x^3-x) in $\mathbf{Q}[x]$.
   (b) Find a generator for the ideal $(2+3\sqrt{-2}, 3-\sqrt{-2})$ in I_{-2}.

9. Let $\mathfrak{p}$ be a proper ideal of a commutative ring R with identity 1_R. Show that the following are equivalent:
   - For all elements $a, b \in R$, $ab \in \mathfrak{p}$ implies $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.
   - For all ideals $\mathfrak{a}, \mathfrak{b}$ in R, $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$ implies $\mathfrak{a} \subseteq \mathfrak{p}$ or $\mathfrak{b} \subseteq \mathfrak{p}$.