Some Ring Theory Class Notes

Class March 12

Conventions regarding 1 (multiplicative unity):

1. Every ring R has a multiplicatuve unity denoted by 1 or 1_R such that $1 * a = a * 1 \; \forall \; a \in R$. Note: $1 = 0$ in $R \Leftrightarrow R = \{0\}$ because $\forall a \in R$: $a = a * 1 = a * 0 = 0$.
2. Any subring S of R must contain 1_R. For subring, check
   (a) $1_R \in S$
   (b) $a \in S \implies -a \in S$
   (c) $a, b \in S \implies a + b \in S$
   (d) $a, b \in S \implies ab \in S$

   Note: An ideal I of R is a subring if and only if $I = R$ ($1 \in I \implies a = a * 1 \in I \; \forall \; a \in R$).

   Example 0.1. $R \times \{0\} = \{(a, 0) \mid a \in R\}$ is not a subring of $R \times R$ if $R \neq \{0\}$ since $(1, 1) \notin R \times \{0\}$. But $\{(a, a) \mid a \in R\}$ is a subring of $R \times R$.
3. For any ring homomorphism $\varphi : R \to S$ we require $\varphi(1_R) = 1_S$. Note that this is not a consequence of the other ring homomorphism properties:
   (a) $\varphi(a + b) = \varphi(a) + \varphi(b) \; \forall a, b \in R$
   (b) $\varphi(ab) = \varphi(a)\varphi(b) \; \forall \; a, b \in R$

   $\varphi(0) = 0$ is a consequence of (a): $\varphi(0) = \varphi(0+0) = \varphi(0)+\varphi(0) \implies 0 = \varphi(0)$. For multiplication, $\varphi(1) = \varphi(1 * 1) = \varphi(1) * \varphi(1)$ does not necessarily imply $1 = \varphi(1)$ since $\varphi(1)$ need not have a multiplicative inverse in S.

   Example 0.2. $\varphi : R \to R \times R$ which maps $a \to (a, 0)$ is NOT a ring homomorphism since $\varphi(1_R) = (1_R, 0) \neq 1_{R \times R}$ if $R \neq \{0\}$

   Example 0.3. $\psi : R \to R \times R$ which maps $a \to (a, a)$ is a ring homomorphism.
4. For an integral domain R (commutative without zero divisors) we also require $1 \neq 0 \Leftrightarrow R \neq \{0\}$ (neither integral domain nor a field)

   Example 0.4. (a) of fields: $\mathbb{R}, \mathbb{Z}_p$ (p prime), $\mathbb{Q}, \mathbb{C}$. $\mathbb{Q}(\sqrt{2}) := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ subfield of $\mathbb{R}$. Check: $0 \neq x \in \mathbb{Q}(\sqrt{2}) \implies x^{-1} \in \mathbb{Q}(\sqrt{2})$ (need $\sqrt{2} \notin \mathbb{Q}$).
   (b) of integral domains which are no fields: $\mathbb{Z}$, when n is a prime $\implies$ $\mathbb{Z}_n$ is an integral domain, but also a field. When n is not a prime $\implies$ $\mathbb{Z}_n$ has zero divisors and isn't an integral domain. Specifically $\exists \; l, m \in \mathbb{N}$, $1 < l, m < n$ such that $n = lm \rightsquigarrow$ (modulo n). $[0] = [n] = [lm] = [l][m]$ in $\mathbb{Z}_n$ (such that $[l] \neq [0]$ and $[m] \neq [0]$.
   (c) $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ subring of $\mathbb{C}$; $\mathbb{Z}[\sqrt{2}]$ is a subring of $\mathbb{R}$.
   (d) commutative rings which are not integral domains. $\mathbb{Z}_n$, n is not prime. $\mathbb{Z} \times \mathbb{Z}$ has zero divisors e.g. $(1, 0) * (0, 1) = (0, 0)$.
   (e) of non-commutative rings:

i. $M(n, R)$, $n \geq 2$ and R any ring $\neq \{0\}$. $\exists A, B \in M(n, R)$ such that $AB \neq BA$

ii. Hamilton's quaternions $\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$ ($\cong \mathbb{R}^4$ as abelian group). Multiplication is induced by that $\mathbb{Q}$ and distributive laws $\rightsquigarrow$ example of skew field or division ring.

Class March 14

Remark 0.5. Units. $(R* =)\ U(R) := \{a \in R \mid \exists\ b \in R \text{ s.t. } ab = ba = 1\}$

1. There can only be one $b \in R$ with $ab = ba = 1$. In fact, if $ba = 1 = ab = ab'$ for some $b' \in R$ $\implies (ba)b = (ba)b' \implies 1b = 1b' \implies b = b'$. Notation: $a \in U(R)$ $ab = ba = 1 \rightsquigarrow b = a^{-1}$ multiplicative inverse.

2. For non-commutative R, $ab = 1$ usually does not imply $ba = 1$. However, if $\exists c \in R$ with $ca = 1$, then $c = b$ and hence also $ba = 1$. This is seen by $c = c * 1 = c(a * b) = (ca)b = 1 * b = b$.

3. $U(R)$ is closed under multiplication and $(ab)^{-1} = b^{-1}a^{-1}$ for $ab \in U(R)$. Immediately checks that $(U(R), *)$ is a group.

4. $a, b \in R$ are called zero divisors if $a, b \neq 0$ but $ab = 0$. $U(R) \cap \{\text{zero divisors}\} = \emptyset$.

Example 0.6. 1. F field (or skew field) $\implies U(F) = F \setminus \{0\} =: F*$

2. $U(\mathbb{Z}) = \{1, -1\}$. $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \implies U(\mathbb{Z}[i]) = \{1, -1, i, -i\} = \{x \in \mathbb{Z}[i] \mid |x| = 1\}$

3. $U(\mathbb{Z}_n) = \{[a] \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$. Notation $U(\mathbb{Z}_n) = U(n)$.

4. $U(R \times S) = U(R) \times U(S)$ (direct product groups). $(a, b) \implies (a, b)^{-1} = (a^{-1}, b^{-1})$.

5. $U(M(n, F)) = GL(n, F) = \{A \in M(n, F) \mid det(A) \neq 0\}$

Remark 0.7. The Center (of a Ring). $Z(R) := \{z \in R \mid za = az\ \forall\ a \in R$. This is a subring of R:

1. $1 \in Z(R)$ since $a * 1 = 1 * a = a\ \forall\ a \in R$

2. $z \in Z(R) \implies -z \in Z(R)$: $-z * a = -(za) = -(az) = a * (-z)\ \forall\ a \in R$.

3. $y, z \in Z(R) \implies y + z \in Z(R)$: $(y + z)a = ya + za = ay + az = a(y + z)\ \forall a \in R$.

4. $y, z \in Z(R) \implies yz \in Z(R)$. $(yz)a = y(za) = y(az) = (ya)z = (ay)z = a(yz)\ \forall\ a \in R$.

Remark 0.8. Integral Multiples (of element of R). For $a \in R$, $n \in \mathbb{Z}$, we define $n * a :=$ if $n > 0, a + ... + a$, if $n = 0$, 0 n-times and if $n < 0$, $(-a) + ... + (-a)$ n-times.
Note: $n > 0$: $a + ... + a = 1_R a + ... + 1_R a$. $a(1_R + ... + 1_R) = (n * 1_R)a$. If $n < 0$, $n * a = (-a) + ... + (-a) = ((-1_R) + ... + (-1_R))a = (n * 1_R)a$. Always, $n * a = (n * 1_R)a\ \forall\ a \in R\ \forall\ n \in \mathbb{Z}$.

Remark 0.9. More rules:

1. $a \in Z(R)$ (e.g. $a = 1_R$), then $n * a \in Z(R)\ \forall\ n \in \mathbb{Z}$ since $Z(R)$ is a subring of R.

2. $(-n) * a = -(n * a)\ \forall\ n \in \mathbb{Z}$, $a \in R$

3. $1 * a = a \; \forall \; a \in R$ by definition

4. $n * (a + b) = n * a + n * b \; \forall \; n \in \mathbb{Z} \; \forall \; a, b \in R$ (follows from $(R, +)$ is an abelian group).

5. $(n + m) * a = n * a + m * a$

6. $(nm) * (ab) = (n * a)(m * b) \; \forall \; n, m \in \mathbb{Z} \; \forall \; a, b \in R$.

7. $(nm) * a = n * (m * a) \; \forall \; n, m \in \mathbb{Z}, \; \forall \; a \in R$.

Definition 0.10. For any ring R, there is a unique ring homomorphism $\varphi = \varphi_R : \mathbb{Z} \to R$ which maps $1 \to 1_R$. Must have $\varphi(1) = 1_R$.
If $n \in \mathbb{Z}$, $n > 0$ then $\varphi(n) = \varphi(1 + ... + 1) = \varphi(1) + ... + \varphi(1) = 1_R + ... + 1_R = n * I_R$. $n \in \mathbb{Z}$, $n < 0$, then $\varphi(n) = -\varphi(-n) = -\varphi(1 + ... + 1) = -(-n * 1_R) = n * I_R$. Therefore, the only possible ring homomorphism is $\varphi_R : \mathbb{Z} \to R$ (which maps $n \to n * 1_R$) $\ni \varphi(n) = n * 1_R \; \forall \; n \in \mathbb{Z}$.
Now, we check $\varphi : \mathbb{Z} \to R$ which maps $n \to n * I_R$ is in fact a ring homomorphism:

1. $\varphi(1) = 1_R$ by definition

2. $\varphi(n + m) = (n + m)1_R = n * 1_R + m * 1_R = \varphi(n) + \varphi(m) \; \forall \; n, m \in \mathbb{Z}$.

3. $\varphi(n * m) = (nm)1_R = (nm)(1_R * 1_R) = n1_R * m1_R = \varphi(n)\varphi(m) \; \forall \; n, m \in \mathbb{Z}$.

Note: φ ring hom $\implies \varphi(\mathbb{Z}) = \{n * 1_R \mid n \in \mathbb{Z}\}$ is a subring of R. Moreover, $\varphi(\mathbb{Z}) \subseteq Z(R)$ since $n * 1_R \in Z(R) \; \forall \; n \in \mathbb{Z}$. The kernel of φ_R is an ideal of $\mathbb{Z}$. Hence, $Kern(\varphi_R) = n\mathbb{Z}$ for a unique $n \in \mathbb{N}_0$.

Definition 0.11. The characteristic of R is defined as $char(R) = n \in \mathbb{N}_0$ with $Kern(\varphi_R) = n\mathbb{Z}$. Alternatively, $char(R) = 0 \Leftrightarrow m * 1_R \neq 0 \; \forall \; m > 0$. $char(R) = n > 0 \Leftrightarrow n * 1_R = 0$ and $m * 1_R \neq 0 \; \forall \; 1 \leq m < n$.

Class March 16

Remark 0.12. Some review! For any given ring R with 1, $\exists$ unique ring homomorphism $\varphi_R : \mathbb{Z} \to R$ which maps $m \to m * 1_R$. It is important to note that $\varphi_R(\mathbb{Z})$ is a subring of R, $\varphi_R(\mathbb{Z}) \subseteq Z(R)$, and $Kern(\varphi_R)$ is an ideal of $\mathbb{Z} \implies \exists$ unique $n \in N_0$ with $Kern(\varphi_R) = n\mathbb{Z}$. (For notation purposes, $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$)

Definition 0.13. If $Kern(\varphi_R) = n\mathbb{Z}$, $n \in \mathbb{N}_0$, then n is called the characteristic of R, $char(R) = n$. An alternative characterization:

1. $m * 1_R \neq 0 \; \forall \; m \in \mathbb{N} \Leftrightarrow char(R) = 0$

2. n is the smallest natural number with $n * 1_R = 0 \Leftrightarrow char(R) = n$.

Example 0.14.

1. $char(\mathbb{Z}) = 0$ ($\varphi_{\mathbb{Z}} = id_Z$) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all fiels of characteristic 0 and $char(\mathbb{Z}[i]) = 0$

2. $char(\mathbb{Z}_n) = n \; \forall \; n \in \mathbb{N}$ and $\varphi_{\mathbb{Z}_n} : \mathbb{Z} \to \mathbb{Z}_n$ which maps $m \to [m]$

3. if p is prime, then $\mathbb{Z}_p$ is a field of characteristic p.

Remark 0.15. If S is a subring of R, then $char(S) = char(R)$

Proof. $1_S = 1_R \implies \varphi_S(m) = \varphi_R(m) = m * 1_R \; \forall \; m \in \mathbb{Z} \implies char(S) = char(R)$ $\square$

Definition 0.16. Any ring R has a unique smallest subring called the prime subring R_0 of R, namely $R_0 = \varphi_R(\mathbb{Z}) = \{m{*}1_R \mid m \in \mathbb{Z}\}$ and any subring of R must contain 1_R and hence $\{m{*}1_R \mid m \in \mathbb{Z}\} = R_0$

Theorem 0.17. *1st Isomorphism Theorem for Rings: If $\varphi : R \to S$ is a ring homomorphism, then $Kern(\varphi)$ is an ideal of R and $R/Kern(\varphi) \cong \varphi(R)(\subseteq S)$.*

Proof. On the level of abelian groups, the map $\hat{\varphi} : R/Kern(\varphi) \to \varphi(R)$ which maps $a + Kern(\varphi) \to \varphi(a)$. This map is a well-defined isomorphism (see 1.2.2). We want a ring homomorphism. Therefore, we have to check that $\hat{\varphi}$ is also multiplicative. $\hat{\varphi}((a+K)(b+K)) = \hat{\varphi}(ab+K) = \varphi(ab) = \varphi(a)\varphi(b) = \hat{\varphi}(a+K)\hat{\varphi}(b+K)$ □

Proposition 0.18. *R ring with prime subring R_0. If $char(R) = 0$, then $R_0 \cong \mathbb{Z}$. If $char(R) = n > 0$, then $R_0 \cong \mathbb{Z}_n$*

Proof. $\varphi_R : \mathbb{Z} \to R$ with $Kern(\varphi_R) = n\mathbb{Z}$ for $n \in \mathbb{N}_0$, $n = char(R)$. $R_0 := \varphi_R(\mathbb{Z}) = \mathbb{Z}/Kern(\varphi_R) = \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}$ if $n < 0$ and $\mathbb{Z}_n$ if $n \geq 0$ □

Remark 0.19. R is an integral domain $\to$ By definition, R is commutative (w/ $1 \neq 0$).

Corollary 0.20. *If R is an integral domain, then either $char(R) = 0$ or $char(R)$ is a prime number.*

Proof. R_0, as a subring of an integral domain must be an integral domain itself. But by the previous proposition, $R_0 \cong \mathbb{Z} \implies char(R) = 0$ (integral domain) or $R_0 \cong \mathbb{Z}_n$ with $char(R) = n$, but $\mathbb{Z}_n$ is an integral domain $\Leftrightarrow$ n is prime (implies zero divisors). $a, b \in R$ are zero divisors $\Leftrightarrow$ $a \neq 0$ and $b \neq 0$ and $ab = 0$ $n = ml$, $1 < m, l < n \implies [m], [l]$ are zero divisors in $\mathbb{Z}_n \implies [m][l] = [n] = [0]$. □

Ideals. R ring with 1.

Definition 0.21. Repetition. A subset $I \subseteq R$ is called an ideal of R of (1) $0 \in I$ (2) $a, b \in I \implies a + b \in I$ (3) $r \in R$, $a \in I \implies ra, ar \in I$.

Remark 0.22. $a \in I \implies$ by (3) $(-1)a = -a \in I$. Hence, $(I, +)$ is a subgroup of the abelian group $(R, +)$. Notation: $I \lhd R$ means that I is an ideal of $R \rightsquigarrow$ quotient ring R/I such that $+ : (a+I) + (b+I) := (a+b) + I$ $(a, b \in R)$ and $* : (a+I) * (b+I) := ab + I$. These operations are well-defined and yield a (quotient) ring $(R/I, +, *)$. $0_{R/I} = I = (0 + I)$ and $1_{R/I} = 1 + I$.
Why is $*$ well-defined? Assume $a + I = a' + I$, $b + I = b' + I \implies a' = a + x$ for some $x \in I$ and $b' = b + y$ for some $y \in I$. $a'b' = (a+x)(b+y) = ab + (ay + xb + xy) \implies$, by $(ay + xb + xy) \in I$, $a'b' + I = ab + I$.

Lemma 0.23. *$\varphi : R \to S$ is a ring homomorphism.*

1. *if $J \lhd S$, then $\varphi^{-1}(J) \lhd R$*
2. *if $I \lhd R$ and φ is surjective, then $\varphi(I) \lhd S$*

Remark 0.24. (2) is not true without surjectivity e.g. $\varphi : \mathbb{Z} \to \mathbb{Q}$ which maps $m \to m$ and $n\mathbb{Z} \lhd \mathbb{Z}$ but $n\mathbb{Z} \ntriangleleft \mathbb{Q}$ (unless $n = 0$.

Proof. Proof of (1).

1. $0_S \in J \lhd S$ and $\varphi(0_R) = 0_S \implies 0_R \in \varphi^{-1}(J)$
2. $a, b \in \varphi^{-1}(J) \implies \varphi(A), \varphi(B) \in J \implies \varphi(a+b) = varphi(a) + \varphi(b) \in J \implies a + b \in \varphi^{-1}(J)$

3. $a \in \varphi^{-1}(J)$, $r \in R \implies \varphi(a) \in J \implies varphi(ar) = \varphi(a)\varphi(r) \in J$, $\varphi(ra) = \varphi(r)\varphi(a) \in J \implies ar \in \varphi^{-1}(J)$ and $ra \in \varphi^{-1}(J)$

$\square$

Remark 0.25. In particular, $Kern(\varphi) = \varphi^{-1}(\{0\})$ is an ideal of R.